(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1656773 B
(45)授权公告日 2010.04.28

(21)申请号 03811865.3
(22)申请日 2003.05.23
(30)优先权数据
02011440.1 2002.05.24 EP
(85)PCT申请进入国家阶段日
2004.11.24
(86)PCT申请的申请数据
PCT/EP2003/005421 2003.05.23
(87)PCT申请的公布数据
WO2003/100544 EN 2003.12.04
(73)专利权人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩
(72)发明人 A·布斯博姆 R·奎内特 M·舒巴 S·霍尔特曼斯
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 刘红 王忠忠
(51)Int.Cl.
H04L 29/06(2006.01)
G06F 1/00(2006.01)
(56)对比文件
CN 1229219 A,1999.09.22, 全文.
WO 01/11450 A1,2001.02.15, 全文.
US 2001/0037469 A1,2001.11.01, 全文.
US 5740361 A,1998.04.14, 全文.
WO 01/82190 A1,2001.11.01, 全文.
审查员 韩晓莉

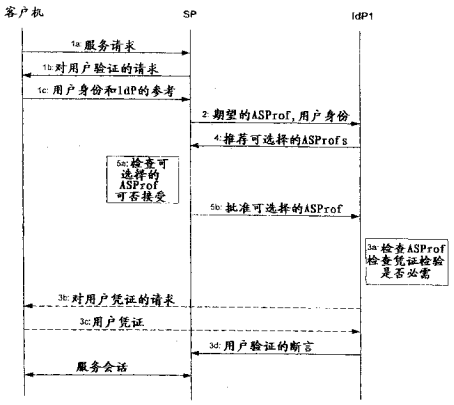
权利要求书 3 页 说明书 24 页 附图 13 页

(54)发明名称

用于对服务供应商的服务验证用户的方法

(57)摘要

公开了用于对服务供应商(SP)的服务验证用户的方法、设备和计算机程序。请求用户到服务供应商(SP)的服务上的访问。由服务供应商(SP)选择一个或多个验证安全简档,用于规定用于对服务验证用户的服务供应商(SP)的验证安全要求。从服务供应商(SP)向身份供应商(IdP1)发送一个或多个选取的验证安全简档的指示和对于身份供应商(IdP1)识别用户的用户身份,以请求身份供应商(IdP1)验证用户。基于用户身份和一个或多个选取的验证安全简档之一来验证用户。把指示对于服务供应商(SP)验证用户的断言发送给服务供应商(SP)。



CN 1656773 B

1. 一种用于对服务供应商 (SP) 的服务验证用户的方法,包括以下步骤 :

请求用户接入到服务供应商 (SP) 的服务,

由服务供应商 (SP) 选择一个或多个验证安全简档,所述一个或多个验证安全简档包括用于规定对服务验证用户的验证安全要求的至少一个安全属性,

把一个或多个选取的验证安全简档的指示和识别用户的用户身份发送给身份供应商 (IdP1),以请求由身份供应商 (IdP1) 验证用户,

基于一个或多个选取的验证安全简档之一和用户身份来验证用户,以及

向服务供应商 (SP) 发送指示用户验证的断言。

2. 按照权利要求 1 的方法,其中服务供应商 (SP) 从一个或多个安全简档的一组中选择被指示为要被身份供应商 (IdP1) 支持用于验证的一个或多个验证安全简档。

3. 按照权利要求 2 的方法,其中服务供应商 (SP) 从身份供应商 (IdP1) 接收用于这组一个或多个被支持的安全简档的指示。

4. 按照权利要求 1-3 之一的方法,其中执行验证所根据的所述一个验证安全简档是由身份供应商 (IdP1) 从选取的验证安全简档中选择的。

5. 按照权利要求 1-3 之一的方法,其中一个或多个选取的验证安全简档利用一个或多个关系被关联到一个或多个其它的验证安全简档上,每个关系表示一个或多个选取的验证安全简档相对一个或多个其它的验证安全简档在验证安全强度上的排序,而且验证用户的步骤通过如下来执行 :

由身份供应商 (IdP1) 选择与一个或多个选取的验证安全简档相比在验证安全强度上相等强度或更大强度相关联的一个或多个其它的验证安全简档之一,以及

基于选取的其它的验证安全简档来验证用户。

6. 按照权利要求 5 的方法,其中服务供应商 (SP) 规定与一个或多个其它的验证安全简档的一个或多个关系,并且服务供应商 (SP) 把与一个或多个其它的验证安全简档的一个或多个关系的指示发送给身份供应商 (IdP1)。

7. 按照权利要求 1 的方法,其中利用执行验证所根据的验证安全简档的指示来补充断言,并且由服务供应商 (SP) 检查指示的验证安全简档是否可以接受。

8. 一种用于对服务供应商 (SP) 的服务验证用户的方法,包括以下步骤 :

请求用户访问服务供应商 (SP) 的服务,

把识别用户的用户身份发送给身份供应商 (IdP1),用于请求由身份供应商 (IdP1) 验证用户,

基于用户身份和验证安全简档来验证用户,所述验证安全简档包括至少一个安全属性,

把指示用户验证的断言发送给服务供应商 (SP),利用验证安全简档的指示来补充此断言,以及

服务供应商 (SP) 检查指示的验证安全简档可接受性。

9. 按照权利要求 1 或 8 的方法,进一步包括以下步骤 :在服务供应商 (SP) 一方接收来自用户设备的用户身份和身份供应商 (IdP1) 的参考信息,以响应从服务供应商 (SP) 向用户设备发送的验证请求。

10. 按照权利要求 1 或 8 的方法,进一步包括以下步骤 :基于该断言准许对所述服务的

访问。

11. 按照权利要求 7 或 8 的方法，进一步包括以下步骤：基于断言和基于通过服务提供商 (SP) 对所述指示的验证安全简档的可接受性的检查来准许对所述服务的访问。

12. 按照权利要求 1 或 8 的方法，进一步包括以下步骤：验证升级，通过基于至少一个其它的验证安全简档执行其它的验证，执行验证升级。

13. 按照权利要求 12 的方法，其中验证升级包括改变为其它的身份供应商 (IdP2)，以便基于其它的验证安全简档来执行其它的用户验证。

14. 一种与服务供应商 (SP) 相关的设备，此设备包括用于接收消息的接收单元、用于发送消息的发射单元和用于处理消息与信息的处理单元，其中此设备适用于：

接收用户对服务供应商 (SP) 的服务的访问请求，

选择一个或多个验证安全简档，所述一个或多个验证安全简档包括至少一个安全属性，用于规定验证安全要求，以便对服务验证用户，

把一个或多个选取的验证安全简档的指示和识别用户的用户身份发送给身份供应商 (IdP1)，用于请求由身份供应商 (IdP1) 验证用户，以及

接收指示由身份供应商 (IdP1) 验证用户的断言。

15. 按照权利要求 14 的设备，其中该设备适用于从一组安全简档中选择被指示为被身份供应商 (IdP1) 支持用于验证的一个或多个验证安全简档。

16. 按照权利要求 15 的设备，其中该设备适用于从身份供应商 (IdP1) 接收用于这组一个或多个被支持的安全简档的指示。

17. 按照权利要求 14-16 之一的设备，其中该设备适用于通过一个或多个关系把一个或多个选取的验证安全简档关联到一个或多个其它的验证安全简档上，所述一个或多个关系的每个关系表示一个或多个选取的验证安全简档相对于一个或多个其它的验证安全简档在验证安全强度上的排序，并且此设备进一步适用于把与一个或多个其它的验证安全简档的至少一个或多个关系发送给身份供应商 (IdP1) 以便验证，其中一个或多个其它的验证安全简档在验证强度上被相等强度或更大强度相关联。

18. 按照权利要求 14-16 之一的设备，其中该设备适用于接收由身份供应商 (IdP1) 执行用户验证所根据的验证安全简档的指示，并且该设备进一步适用于检查指示的验证安全简档的可接受性。

19. 一种与服务供应商 (SP) 相关的设备，该设备包括用于接收消息的接收单元、用于发送消息的发射单元和用于处理消息与信息的处理单元，其中此设备适用于：

接收用户对服务供应商 (SP) 的服务的访问请求，

把识别用户的用户身份发送给身份供应商 (IdP1)，以请求由身份供应商 (IdP1) 验证用户，

接收来自身份供应商 (IdP1) 的指示用户验证的断言，利用包括至少一个安全属性的验证安全简档的指示来补充此断言，以及

检查指示的验证安全简档的可接受性。

20. 按照权利要求 14 或 19 的设备，其中该设备适用于接收来自用户设备的用户身份和身份供应商 (IdP1) 的参考信息，以响应从与服务供应商 (SP) 相关的设备向用户设备发送的验证请求。

21. 按照权利要求 14 或 19 的设备，其中该设备适用于基于断言准许对服务的访问。

22. 按照权利要求 18 或 19 的设备，其中该设备适用于基于断言和基于通过与服务提供商 (SP) 相关的设备、对所述指示的验证安全简档的可接受性的检查来准许对服务的访问。

23. 按照权利要求 14 或 19 的设备，其中该设备适用于基于其它的验证安全简档根据其它的验证执行验证升级。

24. 按照权利要求 14 或 19 的设备，其中该设备适用于为了验证升级而更改到其它的身份供应商 (IdP2)，以便执行其它的验证。

25. 一种与身份供应商 (IdP1) 相关的设备，该设备包括用于接收消息的接收单元、用于发送消息的发射单元和用于处理消息与信息的处理单元，其中此设备适用于：

接收用户验证的请求，此请求包括对于身份供应商 (IdP1) 识别用户的用户身份和用于一个或多个验证安全简档的指示，该一个或多个验证安全简档包括规定服务供应商 (SP) 的验证安全要求的至少一个安全属性，用于对于服务供应商 (SP) 的服务验证用户，

基于一个或多个验证安全简档之一和用户身份来验证用户，以及

向服务供应商 (SP) 发送指示用户验证的断言。

26. 按照权利要求 25 的设备，其中该设备适用于把被身份供应商 (IdP1) 支持用于验证的一组一个或多个安全简档的指示发送给服务供应商 (SP)。

27. 按照权利要求 25 或 26 的设备，其中该设备适用于从验证安全简档中选择执行验证所根据的所述一个验证安全简档。

28. 按照权利要求 25 或 26 的设备，其中利用一个或多个关系把一个或多个验证安全简档和一个或多个其它的验证安全简档相关联，所述一个或多个关系的每个关系表示一个或多个验证安全简档相对于一个或多个其它的验证安全简档在验证强度上的排序，并且其中该设备适用于通过选择一个或多个其它的验证安全简档之一并通过基于选取的其它的验证安全简档验证用户来执行用户的验证，其中所述一个或多个其它的验证安全简档与一个或多个验证安全简档相比在验证安全强度上被相等强度或更强强度相关联。

29. 按照权利要求 28 的设备，其中该设备适用于从服务供应商 (SP) 接收与一个或多个其它的验证安全简档的一个或多个关系的指示。

30. 按照权利要求 25 或 26 的设备，其中该设备适用于利用执行验证所根据的验证安全简档的指示来补充断言。

31. 一种与身份供应商 (IdP1) 相关的设备，此设备包括用于接收消息的接收单元、用于发送消息的发射单元和用于处理消息与信息的处理单元，其中此设备适用于：

接收验证用户的请求，此请求包括相对于身份供应商 (IdP1) 识别用户的用户身份，

基于用户身份和包括至少一个安全属性的验证安全简档来验证用户，以及

向服务供应商 (SP) 发送指示用户验证的断言，利用执行用户验证所根据的验证安全简档的指示来补充此断言。

32. 按照权利要求 25 或 31 的设备，其中该设备适用于执行验证升级，验证升级以其它的验证为基础，所述其它的验证则以其它的验证安全简档为基础。

用于对服务供应商的服务验证用户的方法

技术领域

[0001] 本发明涉及验证领域，并且特别涉及用于对服务供应商的服务验证用户的方法。

背景技术

[0002] 类似于互联网上的网站或电子商务的许多电子可获得的服务为了若干目的而需要用户识别和验证，像提供对机密信息或服务或资源的访问，例如基于 web 的电子邮件访问或者在线银行业务，像提供适应于用户简档的个人化服务，像数据挖掘，即从大量用户与服务之间的交互得出结论，例如为了创建作为消费者的用户行为的简档，或者像在电子商务应用中检验用户信誉这样的目的，例如通过确信用户总是支付其帐单来检验。为了准许对其他形式的服务进行访问可能也需要用户识别和验证，像访问类似于汽车门或公司建筑物或方向盘的物理单元。

[0003] 识别意味着对身份进行规定，身份毫不含糊地定义了某个用户或某组用户。被规定的身份对于特定的一个人或一组人可以是或也可以不是可追踪的，即身份可能是明文形式的用户的名字，但也可能是随机选择的登录名。唯一的要求是在组人登录的情况下特定的一组人中只有单个人或某个人在特定用户身份下注册了，基于此特定用户身份有可能识别注册的用户。举个例子，例如可以是用来访问服务供应商的服务的用户的登录名。验证被定义为对身份进行检验，例如检验呈递某个身份的用户是否实际上就是在该相同身份下初始注册过了的同一个用户。

[0004] 验证是通过检验用户凭证 (credential) 来完成的。基本上有三种类型的用户凭证。首先，用户拥有的东西，例如钥匙、智能卡、护照、公司身份卡等等，其次，用户知道的东西，例如口令、个人识别号码 (PIN)、他妈妈的娘家姓等等，再次，用户的身体特征，例如虹膜图型、语音、指纹、面部特征、笔迹等等。

[0005] 用户验证可以包括对一种或多种类型凭证的检验，例如口令只是与 PIN 代码知识组合拥有公司 ID。例如用户的名字这样的用户身份被用在识别步骤里，以便把进行验证时从用户那收集的用户凭证和与注册的用户身份相关的用户凭证联系起来。通过检验收集的用户凭证与注册的用户凭证是否匹配来检验用户身份，并从而完成验证。因而验证一般包括要求验证作为先决条件的实体的识别，并且用户的注册对验证来说是必需的。

[0006] 过去，每个服务供应商一般执行自己用户的识别和验证，例如最常见的是经由用户名和口令，有可能使用安全传输协议，并留意自己用户简档数据库。对于用户来说缺陷在于他一般得记住对于不同的服务供应商的用户身份和口令的不同组合，或者更普遍的是用户身份和凭证的不同组合，这是不方便的，而且在大多数情况中当用户把他的不同的用户身份和与之对应的各个口令（凭证）写下来时不是非常安全。如果用户对于不用的服务供应商使用相同或相似的组合，安全性就进一步受到威胁。对于服务供应商来说缺陷在于它得保留自己的数据库，并且还得自己执行所有的验证步骤。此外，由于技术和经济原因服务供应商自行验证一般基于单个或很有限数量的用户凭证类型，因为建立适当的基础设施来收集并处理不同类型的用户凭证耗费很大，这对于现代验证方法的引进是严重的障碍，像

基于生物统计学或基于智能卡的方法，智能卡像移动电话里的用户身份模块 (SIM) 卡。

[0007] 近来，已经出现了若干技术，例如Microsoft® Passport（微软®口令），请见例如 2001 年三月在 http://www.passport.com 上公布的 Microsoft PassportTechnical White Paper（微软口令技术白皮书），目标是把验证从实际服务中分离出来。这样的话，“身份供应商”（“IdP”）负责用户注册以及，无论何时用户想访问服务时都负责用户验证。可以在单个实体内完成用户注册和用户验证，并且也可以把两者分开。实际服务的供应商（“服务供应商”，“SP”）与身份供应商可以是同一个也可以不是同一个。身份供应商可能本身充当某些服务的供应商，此外也可能对外部服务供应商提供身份服务。在Microsoft® Passport 中，用户验证总是经由用户名 / 口令机制来完成，经由 SSL 来传输，而对口令改变间隙没有任何限制，从而可以访问向Microsoft® Passport 注册过的任何种类的服务。

[0008] 身份供应商和服务供应商的功能性的分离有若干优点：服务供应商不必管理自己用户的注册和验证，而可以把这些“外源 (outsource)”给身份供应商。然而，更重要的是用户能够只利用一个一致的登录流程到达不同服务。正如所述，现今的用户必须要记住并且 / 或者拥有各个服务供应商之间相互独立的验证凭证，或者重新使用像口令这样的凭证，这当然对安全有威胁。比如，一个攻击者可能窃听用户在 web 门户输入的未加密的口令，并且然后使用它试图访问有相同口令的用户在线银行账户。

[0009] 然而，已知的身份供应商的解决方案Microsoft® Passport 不区分不同服务或服务供应商的不同安全要求。服务供应商的安全要求主要取决于需要进行验证的目的。为了单纯提供个人化的 web 门户，除了对银行账户进行在线访问或者对主要的现金交易进行授权，有较低的安全等级也就足够了。更确切地说，Microsoft® Passport 认为验证是二元判定，就像只基于一种凭证类型被验证或未被验证，并且假定基于用户名 - 口令组合的静态验证机制是身份供应商和服务供应商都知道的并预先 - 明显地或隐含地 - 认同了。这显然有若干缺点，包括，首先不能应付不同服务 / 资源的不同类型的安全要求，也不能应付随着时间的过去在安全要求上的改变。如果护照类的身份供应商决定改变验证处理，这就需要独立地使用频带外装置把这告知每个服务供应商，或者服务供应商只得希望身份供应商实行的任何改变都是“合理的”。

[0010] WO 01/11450 公开了一种单个符号验证多个信息资源的系统结构和方法。安全结构把信任等级要求与信息资源关联起来，并且基于口令、证书、生物统计学技术和智能卡的验证方案与信任等级相关。一旦收到访问信息资源的请求，不用先验证信任等级是否足够，介于客户机实体和信息资源之间的看门人 (gatekeeper) 就按照映射规则使用凭证收集服务来获得客户机实体的登录凭证，此映射规则在足够的信任等级和一套合适的凭证类型之间建立起对应关系。

[0011] 在 WO 01/11450 A1 中说明的系统有若干局限性。首先，它依靠信息资源和信任等级之间的关联以及信任等级和用来进行验证的凭证类型之间的映射规则，既要事先知道又要事先认同提供了身份供应商功能性的实体和信息资源之间的关联和映射规则。而且，与同一信任等级相关的所有信息资源都以同样的方式来处理。无论何时身份供应商决定改变关联和 / 或映射规则，这就特别成问题，因为不是所有受到改变影响的信息资源（或各个信息资源的供应商）例如由于安全、技术或商业有关原因可以发觉改变可以接受。从而，最终不是信息资源的供应商和信息资源本身而是身份供应商确定验证处理，即确定哪个特定凭

证是准备用于特定验证。

[0012] 然而，由身份供应商做出的这种方针决策是许多服务供应商不能接受的。从而对关联和映射规则进行更新会造成与服务供应商之间的冲突。静态或预定的关联或映射规则不够灵活，满足不了有关实体的要求。此外，用预定的关联或映射规则表示验证方案和凭证类型所有可能出现的组合来满足所有的服务供应商和所有类型的服务的各种安全要求，这是相当复杂的，尤其是鉴于验证方法数量和种类的增加以及服务供应商有时快速变化着的要求。由于对这么多种可能性来说预定的关联或映射规则存在固有的不灵活性，所以只要有可能，在能够按照新的安全要求验证之前得对关联或映射规则执行麻烦的更新操作。在特别情况下这种不灵活性尤其是个缺陷，例如在请求访问与任何或有效的信任等级无关的例如新引进的服务时。另一个的局限性在于客户机和所访问的信息资源之间进行会话期间包括请求和响应在内的所有信息流都经过作为进入路径部件的看门人。然而，使用身份供应商作为进入路径部件来传送用户客户机和服务供应商之间的整个信息流不必要地增加了身份供应商的负载。

[0013] Microsoft® Passport 和 WO 01/11450 A1 共同的另一局限性是只有一个身份供应商被用于验证目的。这种限制迫使用户和服务供应商只信任一个身份供应商。然而，因为隐私、信任、商业和费用的原因，集中式的验证事例常常不被用户和服务供应商所接受。比如，用户不想让用户有关信息只在一个身份供应商上就被采集到，用户有关信息像各种类型的凭证，以免不必要的数据聚集或甚至欺诈。

发明内容

[0014] 本发明的一个目的是提供以更加安全和灵活的方式对服务供应商的服务验证用户的方法、设备和计算机程序。

[0015] 通过权利要求 1 和 9 中所述的方法而达到这个目的。而且，此发明体现在权利要求 15、21、27 和 34 中所述的设备和权利要求 36 和 37 中所述的计算机程序上。有利的实施方案在其他的权利要求中陈述。

[0016] 公开了一种对服务供应商的服务验证用户的方法。

[0017] 此方法可以通过用户请求访问服务供应商的服务来启动。从用户的设备向服务供应商发送此请求，触发服务供应商利用下面的步骤继续运行。或者，请求可以被预先设置并在例如预定时间或间隔上到达服务供应商。

[0018] 一旦被访问请求触发，服务供应商就选择一个或多个验证安全简档来规定对服务验证用户的验证安全要求。

[0019] 方法继续进行，通过把一个或多个选取的验证安全简档的指示和识别用户的用户身份发送到身份供应商来请求身份供应商验证用户，即服务供应商从其相关的设备或例如服务供应商可以远程访问的设备上发送一个或多个选取的验证安全简档作为一种形式的指示，以一个或多个验证安全简档的形式向身份供应商指示验证安全要求，在这些简档之一的基础上准备执行验证。此外，向身份供应商发送用户身份，是为了验证步骤进行用户识别这个目的。

[0020] 接着，基于用户身份以及一个或多个选取的验证安全简档之一，用户被身份供应商验证。通过识别用户和检验用户来完成验证，例如识别用户是否为先前向身份供应商所

注册的那个，并按照这一个验证安全简档在用户身份的基础上检验用户。

[0021] 最后，可以把关于身份供应商验证结果的信息发送到服务供应商。尤其是，把指示进行用户验证的断言（assertion）发送到服务供应商，例如，用来指示用户验证已经按照服务供应商的验证安全简档所规定的验证安全要求完成了。取决于实施或使用情况，此断言可以例如规定一个用来进行验证的验证简档或者单纯指示“验证成功”。断言的其他实现方式也是有可能的。

[0022] 此方法改进了对服务供应商的服务进行用户验证的方法并使此方法对服务供应商来说极安全，因为是服务供应商而不是身份供应商最终确定身份供应商要满足的安全要求，从而按照服务供应商所选择的验证安全简档之一验证用户。此方法对身份供应商来说也更安全了，因为它可以清晰地并在传输（on-the-fly）中被指示，服务供应商的哪个验证要求目前适用并且对于目前进行的用户验证必须被满足。服务供应商的验证安全要求可以改变。在这种情况下，服务供应商通过选择另一个验证安全简档会马上适应其改变了的安全要求，从而使此方法对服务供应商来说更安全而且非常灵活。从而，尤其在服务供应商的验证安全要求改变了的特别情形下而且在其他情况和环境下，当身份供应商请求验证时，服务供应商可以灵活行动，并且可以马上规定它改变了的验证要求并用一个或多个选取的验证简档传送给身份供应商。而且，此方法不需要服务供应商只利用特定的单个身份供应商。取而代之，任何身份供应商都可以被用来进行验证。此外，不需要有身份供应商作为介于服务供应商和客户机之间的进入路径（in-path）部件。

[0023] 按照优选实施方案，一个或多个验证安全简档包括至少一个安全属性，用来例如更精确地规定验证安全要求。服务供应商通过规定安全属性可以汇编一个或多个验证安全简档。通过由它自己作规定，服务供应商可以把验证安全简档修整得正好适合它的安全要求。可选择地或者此外，服务供应商可以选择预定的验证安全简档，它包括用预定方式安排的一个或多个安全属性。当规定和／或选择基于一个或多个安全属性的验证安全简档时，就要把身份供应商和／或用户的验证能力考虑进来。安全属性的范例是对凭证、传输层安全性、网络安全性、链接层安全性、定时信息、策略、诈骗检测测量、赔偿责任和／或担保以及其他安全特征这一组中的一项进行说明的规定。安全属性可以包括类型的规定，例如像口令或生物统计学这样的凭证类型，也可以包括与特定类型相关的值的规定，例如与口令相关的口令长度或与生物统计学相关的某个清晰度的指纹。使用安全属性，身份供应商可以得到服务供应商的有关身份供应商按照服务供应商的要求执行用户验证必须基于哪一些安全特征的精确指示。

[0024] 按照另一个优选实施方案，服务供应商从一个或多个安全简档的一组中选择被指示为被身份供应商支持用来验证的一个或多个验证安全简档。从一个或多个被支持的验证安全简档这一组中选择一个或多个验证安全简档增加成功验证的概率。

[0025] 按照另一个优选实施方案，服务供应商接收来自身份供应商的对这组一个或多个被支持的安全简档的指示，例如通过发送被支持的验证安全简档的列表。这个指示也可以是指向服务器的URI，其中可以从此服务器中获得这组简档，例如由服务供应商下载而获得。其他方式的指示也有可能。优选地，在身份供应商的验证能力发生改变时，把对这组简档的指示或这组简档本身作为一种形式的指示发送到服务供应商，例如当身份供应商从被支持的项目中废除某个安全属性时，像废除凭证类型和／或凭证值，例如不再支持短于4个

字符的口令长度，或者假如身份供应商提供新引进的凭证类型或值，例如从今天起指纹被支持。

[0026] 按照另一个优选实施方案，执行验证所基于的所述一个验证安全简档是被身份供应商从一个或多个选取的验证安全简档中选择的。通过这样做，身份供应商可以避免询问服务供应商准备执行的验证是基于选取的验证安全简档中的哪一个。取而代之，身份供应商可以假定所有选取的和指示的验证安全简档都满足服务供应商的验证安全要求，并可以选择最合适的一个，例如最适合于身份供应商和/或得被验证的用户的需要或能力。而且，服务供应商和身份供应商之间为了协商实际执行用户验证是基于哪个验证安全简档而进行的交互作用可以被最小化，并因而成功验证的速度和概率都增加了。

[0027] 按照另一个优选实施方案，一个或多个选取的验证安全简档可以利用一个或多个关系来相关联一个或多个其它的验证安全简档。这些关系中每一个都表示一个或多个选取的验证安全简档相对一个或多个其它的验证安全简档在验证安全强度方面的排序。关系的范例是有向边线 (edge)，表示例如强度大于或等于两个验证安全简档之间的关系。也可以把选取的验证安全简档互相关联起来。基于一个或多个选取的验证安全简档和一个或多个其它的验证安全简档的关系，即，与选取的和其他的验证简档的总体以及各个关系有关的信息，通过由身份供应商选择一个或多个其他的验证安全简档之一并且基于身份供应商选取的这个其他的验证安全简档来验证用户，一个或多个其它的验证安全简档与一个或多个选取的验证安全简档比较在验证安全强度上被相等强度或更强相关联，从而基于一个或多个选取的验证安全简档之一可以执行验证用户的步骤。从而，满足服务供应商的验证安全要求的验证安全简档的种类和数量扩大了。从扩大的种类和数量的验证安全简档之中，身份供应商可以灵活选择一个验证简档用来进行验证，例如最合适前面所解释的某个能力的一个，从而增加成功验证的可能性和验证的速度。

[0028] 按照另一个优选实施方案，服务供应商可以规定到一个或多个其它的验证安全简档的一个或多个关系，并且服务供应商可以把到一个或多个其它的验证安全简档的一个或多个关系的指示发送给身份供应商。通过这样做，一个或多个选取的与一个或多个其它的验证安全简档之间的关系更精确地反映了服务供应商的验证安全要求，这可以导致更快的验证，而对于实际用来进行验证的验证安全简档的协商的交互更少。

[0029] 按照另一个优选实施方案，利用执行验证所基于的验证安全简档的指示来补充断言，并且服务供应商检查指示的验证安全简档是否可以接受。给服务供应商提供与执行验证所基于的验证安全简档有关的信息进一步增加了服务供应商的安全性并给服务供应商提供了例如检查实际上被用来进行验证的验证安全简档是否满足其当前验证安全要求的可能性，。

[0030] 公开了一种对服务供应商的服务验证用户的方法。此方法包括以下步骤：用户请求访问服务供应商的服务；把识别用户的用户身份发送给身份供应商，以请求身份供应商验证用户；基于用户身份和验证安全简档来验证用户；把指示进行用户验证的断言发送给服务供应商；利用验证安全简档的指示来补充此断言；以及服务供应商检查指示的验证安全简档是否可以接受。

[0031] 在此，服务供应商不在进行验证前预先提供它的安全验证要求给身份供应商，这对某些实施方式来说可能是有利的。然而，通过检查执行用户验证所基于的指示的验证安

全简档，相对于服务供应商的安全要求，服务供应商仍然能够检验对用户的服务验证与服务供应商的验证安全要求是否匹配。而且，由于基于被身份供应商支持的任何验证安全简档而进行的验证能够用于验证的事实，验证最好与用户的验证能力相匹配，如果凭证检验有必要的话，所以身份供应商的灵活性增加了。最终，是服务供应商有权决定用户是否被充分验证了。

[0032] 两种方法都可以进一步包括依稀步骤：在服务供应商上接收来自用户设备的用户身份和身份供应商的参考，以响应从服务供应商向用户设备发送的验证请求。这种与用户设备之间进行的交互是很平常的，并且可以轻松地完成此实现方式。

[0033] 基于收到的断言，可以准许基于此断言的对服务的访问。或者，基于断言并基于对可否接受的检查准许服务访问，例如通过检查指示的验证安全简档是否与服务供应商的验证安全要求相匹配，从而验证的安全性增加了，尤其是对于服务供应商来说。

[0034] 按照另一个优选实施方案，此方法可以包括以下步骤：验证升级。通过基于其它的验证安全简档来进行其它的验证，执行验证升级。按照前述的涉及对服务供应商的服务验证用户的方法中的选择和验证的步骤之中的任何步骤，执行选择和其它的验证，例如服务供应商可以选择一个或多个验证安全简档并把这些简档发送给身份供应商，后者选择其中之一用来验证用户。身份供应商可以基于关系来选择某个验证安全简档，可以向服务供应商指示执行验证所基于的选取的验证安全简档，服务供应商可以例如检查指示的验证安全简档，以查看它是否与其用于验证的验证安全要求相匹配。如果打算访问有更强验证安全要求的服务，升级功能可以使用户和服务供应商继续会话。

[0035] 按照另一个优选实施方案，验证升级可以包括对其它的身份供应商的改变，以便基于其它的验证安全简档执行其它的用户验证，从而在先前的身份供应商不支持按照服务供应商更强的验证安全要求进行的其它的验证简档的情况中例如能够继续进行服务会话。

[0036] 此发明进一步体现在设备上。下面，说明与服务供应商相关的设备和与身份供应商相关的设备。

[0037] 公开了与服务供应商相关的设备。与服务供应商相关的设备包括用于接收消息的接收单元、用于发送消息的发射单元和用于处理消息与信息的处理单元。与服务供应商相关的设备可以用于接收用户对服务供应商服务的访问请求，选择一个或多个验证安全简档用来规定验证用户到服务上的验证安全要求，把对一个或多个选取的验证安全简档的指示和识别用户的用户身份发送给身份供应商，以请求身份供应商验证用户，以及接收身份供应商指示用户验证的断言。

[0038] 按照优选实施方案，与服务供应商相关的设备可以用于选择一个或多个验证安全简档，这些简档包括至少一个安全属性，用来规定验证安全要求。

[0039] 按照另一个优选实施方案，与服务供应商相关的设备可以用于从一组安全简档中选择被指示为被身份供应商支持验证的一个或多个验证安全简档。

[0040] 按照另一个优选实施方案，与服务供应商相关的设备可以用于从身份供应商接收对这组一个或多个被支持的安全简档的指示。

[0041] 按照另一个优选实施方案，与服务供应商相关的设备可以用于把一个或多个选取的验证安全简档关联到一个或多个其它的验证安全简档上，每个关系都表示一个或多个选取的验证安全简档相对一个或多个其它的验证安全简档在验证安全强度方面上的排序，并

且此设备可以进一步用于把与一个或多个其它的验证安全简档的至少一个或多个关系发送给用来进行验证的身份供应商，这些其它的简档在验证强度上相等强度或更大强度相关。

[0042] 按照另一个优选实施方案，与服务供应商相关的设备可以用于接收由身份供应商执行用户验证所基于的验证安全简档的指示，并且此设备进一步用于检查指示的验证安全简档是否可以接受。

[0043] 可选择地或此外，与服务供应商相关的设备可以用于接收用户对服务供应商服务的访问请求，把识别用户的用户身份发送给身份供应商，以请求身份供应商验证用户，接收来自身份供应商的指示用户验证的断言，此断言被补充以对验证安全简档的指示，检查指示的验证安全简档是否可以接受。

[0044] 按照另一个优选实施方案，与服务供应商相关的设备可以用于接收来自用户设备的用户身份和身份供应商的参考，以响应从与服务供应商相关的设备向用户设备发送的验证请求。

[0045] 按照另一个优选实施方案，与服务供应商相关的设备可以用于基于断言准许访问服务。

[0046] 按照另一个优选实施方案，与服务供应商相关的设备可以用于基于断言和对接受的检查来准许访问服务。

[0047] 按照另一个优选实施方案，与服务供应商相关的设备可以用于基于其它的验证安全简档在其它的验证基础上执行验证升级。

[0048] 按照另一个优选实施方案，与服务供应商相关的设备可以用于为了验证升级而改变成其它的身份供应商来执行其它的验证。

[0049] 公开了与身份供应商相关的设备。与身份供应商相关的设备包括用于接收消息的接收单元、用于发送消息的发射单元和用于处理消息与信息的处理单元。与身份供应商相关的设备可以用于接收用户验证的请求。此请求包括对于身份供应商识别用户的用户身份，例如识别与身份供应商相关的设备，还包括对于一个或多个验证安全简档的指示，一个或多个验证安全简档为了对服务供应商的服务验证用户而规定了服务供应商的验证安全要求。与身份供应商相关的设备可以进一步用于基于用户身份和一个或多个验证安全简档之一来验证用户，以及向服务供应商发送指示用户验证的断言。

[0050] 按照优选实施方案，与身份供应商相关的设备可以用于根据在执行验证所基于的某个验证安全简档中所包括的至少一个安全属性来验证用户。

[0051] 按照另一个优选实施方案，与身份供应商相关的设备可以用于把被身份供应商支持用于验证的一个或多个安全简档的一组的指示发送给服务供应商。

[0052] 按照另一个优选实施方案，与身份供应商相关的设备可以用于从一个或多个验证安全简档之中选择执行验证所基于的所述一个验证安全简档。

[0053] 可以利用一个或多个关系把一个或多个验证安全简档相关到一个或多个其它的验证安全简档上。一个或多个关系中每一个都表示一个或多个验证安全简档相对一个或多个其它的验证安全简档在验证强度上的排序。与身份供应商相关的设备可以用于通过选择与一个或多个验证安全简档相比在验证安全强度是相等或更大强度被相关的一个或多个其它的验证简档之一并通过基于选取的其它的验证安全简档来验证用户，从而执行用户验

证。

[0054] 按照另一个优选实施方案，与身份供应商相关的设备可以用于从服务供应商接收对于到一个或多个其它的验证安全简档的一个或多个关系的指示。

[0055] 按照另一个优选实施方案，与身份供应商相关的设备可以用于给断言补充上执行验证所基于的验证安全简档的指示。

[0056] 可替换地或此外，与身份供应商相关的设备可以用于接收对验证用户的请求。此请求包括对身份供应商识别用户的用户身份，例如识别身份供应商的设备。与身份供应商相关的设备可以用于基于用户身份和一个验证安全简档来验证用户，以及向服务供应商发送指示用户验证的断言。给此断言补充上执行用户验证所基于的验证安全简档的指示。

[0057] 按照另一个优选实施方案，与身份供应商相关的设备可以用于基于其它的验证安全简档在其它的验证的基础上执行验证升级。

[0058] 本发明进一步体现在一个或多个计算机程序上。一个或多个计算机程序包括可载入设备的软件代码部分，用于执行此验证方法的步骤中的任何步骤。可以把一个或多个计算机程序保存在计算机可读媒体上。计算机可读媒体可以是在设备内或放在外面的永久性或可再写性存储器。也可以把计算机程序转移到设备上，比如作为信号序列经由电缆或无线链路来转移。

[0059] 尤其，公开了可载入与服务供应商相关的设备中的计算机程序。此计算机程序包括如下的代码：用于处理用户对服务供应商服务的访问请求；选择一个或多个验证安全简档来规定用于对服务验证用户的验证安全要求；启动向身份供应商发送对一个或多个选取的验证安全简档的指示和识别用户的用户身份，以请求身份供应商验证用户；以及处理身份供应商指示用户验证的断言。

[0060] 可选择地，计算机程序可以是这样一种格式，不包括或者跳过涉及选择一个或多个验证安全简档以及向身份供应商发送一个或多个验证安全简档的指示的软件部分，并且取而代之或此外，此计算机程序包括代码，用于检查执行用户验证所基于的指示的验证安全简档是否可以接受，所指示的验证简档连同断言一起被输入计算机程序中。

[0061] 而且，公开了可载入与身份供应商相关的设备中的计算机程序。此计算机程序包括代码：用于处理验证用户的请求，此请求包括对于身份供应商识别用户的用户身份和对于一个或多个验证安全简档的指示，这些简档规定了服务供应商的验证安全要求，用来对于服务供应商的服务进行用户验证；基于用户身份和从服务供应商接收的一个或多个验证安全简档之一执行用户验证；以及启动向服务供应商发送指示用户验证的断言。

[0062] 用计算机程序实现此发明的方法有可能还有其他方式。特别是，此计算机程序可以实现所述方法的任何实施方案。

[0063] 下面参考附图说明本发明的详细的实施方案。

附图说明

[0064] 图 1a 示出了具有属性的验证安全简档的一个范例；

[0065] 图 1b 示出了用于验证安全简档及其相对于验证安全强度的排序的一个范例；

[0066] 图 2 示出了用于在数字属性值和验证安全强度之间映射的范例；

[0067] 图 3 示出了用于验证的第一示范性消息流；

[0068] 图 4 示出了用于验证的第二示范性消息流；

[0069] 图 5 示出了用于验证的第三示范性消息流；

[0070] 图 6 示出了用于验证的第四示范性消息流；

[0071] 图 7 示出了用于验证的第五示范性消息；

[0072] 图 8 示出了用于验证的第六示范性消息流；

[0073] 图 9 示出了用于验证的第七示范性消息流；

[0074] 图 10 示出了用于验证升级的第一示范性消息流；

[0075] 图 11 示出了用于验证升级的第二示范性消息流；

[0076] 图 12 示出了用于实现此方法的设备的一个范例；

[0077] 图 13 示出了用于实行此方法的设备和设备之间的链路的第一范例；

[0078] 图 14 示出了用于实行此方法的设备和设备之间的链路的第二范例；

[0079] 图 15 示出了用于实行此方法的设备和设备之间的链路的第三范例。

具体实施方式

[0080] 验证方法可以由以下三个单元部分组成：第一，用来描述一个或多个验证安全简档 (ASProf) 的数据结构，以及作为结构化的可扩充的可机读集合的 ASProf 之间的可能关系。为了说明此数据结构，使用有向图来表示不同 ASProf 之间的关系，例如“强度大于等于”(≥)。在这个图中，每个节点是一个 ASProf，每个有向边线表示两个 ASProf 之间的一个关系。第二，同意 ASProf 用来对于服务供应商的服务验证用户的方法。服务供应商可以把一个或多个被请求的 ASProf 从某种意义上说就是一张“希望列表 (wish list)”发送给身份供应商，进而后者决定是否遵照并可以制定被使用的一个或多个 ASProf 的可选择建议。与往返发送全部的 ASProf 相反，使用参考和更新可以减少交换的数据。如果第一身份供应商不能满足服务供应商的要求，就可以联系其它的身份供应商来进行验证。第三，用来在会话期间升级 ASProf 的方法；在会话期间升级 ASProf 涉及再次协商 ASProf，并且升级 ASProf 也可能需要新的用户凭证的检验。如果身份供应商不能满足升级的 ASProf，服务供应商就会联系可选择的身份供应商来进行升级。

[0081] 要求具有身份 X 的用户实际上是与这个身份相关的用户，这个判断的确定程度可以根据连续标度 (scale) 看出来，并且取决于多种因素，包括，但不限于：

[0082] - 为了验证而被检验的一个或多个类型的用户凭证，例如口令可以被认为不如与 PIN 代码结合的公司 ID 安全；

[0083] - 当客户机和服务器之间传达验证信息（例如口令）时所使用的传输、网络和链路层的安全性特征，服务器例如 TLS、IPsec。

[0084] - 最近进行验证的时间，例如十秒前输入的 PIN 一般比三天前输入的 PIN 安全得多，因为攻击者可能趁这三天同时未授权访问客户机设备；

[0085] - 用户凭证的长度和复杂性，例如口令或 PIN 的长度，口令只包含字母，而口令只包含至少两个数字和至少两个特殊字符，密钥的长度，等等；

[0086] - 对于管理秘密用户凭证的策略，例如更改口令的频繁程度，多少次改变以后旧口令被重新使用，身份供应商怎样保护秘密用户凭证数据的机密性和完整性；

[0087] - 对于在使用公共秘钥基础设施 (PKI) 的情况下秘钥管理的策略，例如怎样管理

证明的吊销 (revocation),证明的原件是可信的,等等 ;

[0088] - 进行测量以检测欺诈,以及在检测到欺诈的情况下凭证吊销的流程和吊销所需要的时间 ;

[0089] - 为防欺诈身份供应商向服务供应商提供的赔偿责任 (liability)/ 担保 ;

[0090] - 对于检验向身份供应商注册的用户的“真实”身份的策略,例如在网页上输入名字和个人数据被认为不如口令检验安全。

[0091] 在这篇文档中,这些及其他属性的聚集影响用户验证的确定程度,这被称为“验证安全简档”(“ASProf”)。

[0092] 所述 ASProf 被描述为一套属性,例如上面给出的这些属性,带或不带属性值。例如,空的或者默认的 ASProf 会具有未被分配属性值的属性。可以把 ASProf 设想成包括说明处理过程的策略,通过此处理验证凭证被管理、重建、吊销等等。ASProf 的说明最好是可变更的、可扩充的和可机读的。最好是可扩充标记语言 (XML) 用作底层元语言。因为 ASProf 不是封闭的一套数据而是需要适用于像生物统计学这样的不断出现的验证技术和新颖的安全技术,例如密码 (cryptographic) 技术,所以可扩充性是重要的。可扩充性确保可以把将来的属性包括到 ASProf 里,并且作为替换给定 ASProf 的属性的要求,可扩充性还包括可变更性。不同属性之间可能存在关系。

[0093] 图 1a 示出了一个有不同属性的 ASProf A01 的范例,这些属性像 PIN B01、智能卡 B02、生物统计学 B03、传输安全性 B04 和策略 B05。ASProf 可以被扩充用于将来的属性,例如用于包含用来进行验证的将来的技术 B06。

[0094] 可以把属性值分配给 ASProf 的属性,例如这套属性可以是数字的,即“密钥长度”=“128”,“口令最小长度”=“10”,或者是描述性的,例如“传输安全性”=“TLS 隧道效应”或者“传输安全性”=“WTLS”,TLS 是指传输层安全性并且 WTLS 是指无线 TLS。参考图 1a,属性值的安排如下 :

[0095] 属性 属性值

[0096] PIN 10 个字符

[0097] 智能卡 无

[0098] 生物统计学 (例如指纹) 高分辨率 (200 千字节)

[0099] 传输安全性 WTLS

[0100] 策略 无

[0101] 下面在表 A 中示出了另一个用 XML 编码的有属性的 ASProf 的范例,表 A 在后面的文本给出了注释。下面的例子中一些属性之间存在关系。

[0102] <? xml version =" 1.0" ? >

[0103] <ASProf>

[0104] <user_credentials>

[0105] <password> AA1

[0106] <min_length>5</min_length>

[0107] <max_length>10</max_length>

[0108] <max_session_duration>

[0109] <unit>hours</unit>

```
[0110]          <value>8</value>
[0111]        </max_session_duration>
[0112]        <case_sensitive>yes</case_sensitive>
[0113]        <special_chars_required>
[0114]          none
[0115]        </special_chars_required>
[0116]        <digits_required>1</digits_required>
[0117]      </password>
[0118]  </user_credentials>
[0119]  <transport_layer_security>                          AA2
[0120]    <protocol>
[0121]      <type>TLS</type>
[0122]      <MAC>MD5</MAC>
[0123]      <MAC>SHA</MAC>
[0124]      <cipher>DES</cipher>
[0125]      <cipher>3DES</cipher>
[0126]    </protocol>
[0127]    <protocol>
[0128]      <type>SSL>/type>
[0129]    </protocol>
[0130]  </transport_layer_security>
[0131]  <security_policies>
[0132]    <password>                                        AA3
[0133]      <max_validity>
[0134]        <unit>months</unit>
[0135]        <value>6</value>
[0136]      </max_validity>
[0137]      <first_reuse>10</first_reuse>
[0138]      <privacy_policy>
[0139]        http://www.idprovider.com/w3c/p3p.xml
[0140]      <privacy_policy>
[0141]    </password>
[0142]    <PKI>
[0143]      <trusted_CA>Verisign</trusted_CA>              AA4
[0144]      <trusted_CA>RSA</trusted_CA>
[0145]      <trusted_CA>Thawte</trusted_CA>
[0146]    </PKI>                                          AA5
[0147]    <liability>
[0148]      <max_liability>
```

[0149] <unit>USD</unit>

[0150] <value>0.00</value>

[0151] </max_liability>

[0152] </security_policies>

[0153] <user_registration> AA6

[0154] <ID_verification>

[0155] <type>email_confirmation</type>

[0156] </ID_verification>

[0157] <expiration>

[0158] <time>

[0159] <unit>months</unit>

[0160] <value>6</value>

[0161] </time>

[0162] </expriation>

[0163] <renewal>

[0164] <time>never</time>

[0165] </renewal>

[0166] <revocation> AA7

[0167] <guaranteed_revocation_time>

[0168] <unit>minutes</unit>

[0169] <value>30</value>

[0170] </guaranteed_revocation_time>

[0171] </revocation>

[0172] </user_registration>

[0173] </ASProf>

[0174] 表 A :用于以 XML 编码的 ASProf 的范例。

[0175] 表 A 的注释 :

[0176] AA1 :用于用户验证的口令最少 5 个字符最多 10 个字符。直到再次请求验证为止会话持续时间最大为 8 小时。口令是案件敏感的 (casesensitive),不需要包含特殊字符,但是必须包含至少一个数字字符。

[0177] AA2 :TLS 被用来保证传输层的安全,是容许的消息。验证算法是消息摘译算法 (Security Hash Algorithm)5(MD5) 和安全性散列算法 (Data Encrytion Standard)(SHA),容许的加密算法是数据加密标准 (DES),三倍 DES SSL 还被允许代替 TLS 作为传输层的安全协议。

[0178] AA3 :口令必须至少每 6 个月改变一次,直到用过至少 10 个其他口令才可以再用旧口令。在给定的 URL 上可以找到管理用户数据的详细的隐私策略。

[0179] AA4 :Verisign、RSA 和 Thawte 是被相信为原件证明机构。

[0180] AA5 :身份供应商没有假定对于欺诈或盗窃身份的赔偿责任 ($0.00)。

[0181] AA6 :一旦注册,就使用确认电子邮件发送到她的电子邮件地址来确认用户身份。

当此账户有 6 个月没有使用时，注册期满。不要求对注册信息进行定期更新。

[0182] AA7 :如果检测到欺诈和凭证泄漏，则帐户保证在 30 秒内被阻塞（吊销）。

[0183] 最好按验证安全强度把多个 ASProf 联系起来。可以用有向图的方式说明表示 ASProf 列队或排序的关系。在这幅图中，每个节点都是一个 ASProf。此图可以有“根节点”，它可以是空 ASProf，即，没什么安全性。每个有向边线都规定了两个 ASProf 之间的一个关系，例如“≥”关系。这套 ASProf 和 ASProf 之间的关系最好是可变更的、可扩充的和可机读的。最好是 XML 用作底层元语言。

[0184] 特殊情况可以设想，例如此图变成一个 n 维网格（在 n 个属性的情况下）。要是这样，对于每个属性都有独立的关系，而且两个 ASProf 的比较对应于每个属性的独立比较。两个 ASProf 之间比较的例子有≥关系：

[0185] 如果

[0186] 密钥长度 1 ≥密钥长度 2 与口令长度 1 ≥口令长度 2

[0187] 那么

[0188] ASProf1 ≥ ASProf2

[0189] 然而，更常用的图形表示法考虑了复杂得多的规定，例如密钥长度 64 的指纹辨认比密钥长度 256 的口令更安全。当单一体系中使用了完全不同的验证机制时“把苹果与桔子作比较”的情况就要紧了。图形观念比其他概念更常用，并且允许完全不同的验证方法和技术之间的优先表达式，在其他概念中各个属性被独立处置。

[0190] 原则上说每个服务供应商都可以创建此图，并且不同的服务供应商可以使用不同的图。一个服务供应商可以有多个图形，例如用于不同用户或身份供应商或服务的。这反映了一个要求，每个服务供应商最好都能够定义他自己的优选和优先的验证安全特征。第一服务供应商会认为虹膜扫描比关键字更安全。第二服务供应商会认为关键字更安全。当然，这不排除再用“默认”图的可能，如果服务供应商希望这么做的话。

[0191] 在图 1b 中，描绘了一个 ASProf 图的范例。此图包括用点代表的 ASProf A1、A2、A3、A4、A5、A6、A7、A8、A9，用表示两个 ASProf 之间≥关系的箭头把它们连接起来。图 1b 的图示中所用的箭头符号意思是连接两个 ASProf 的箭头利用其箭头头部指示了两个 ASProf 之一与另一个 ASProf 相比是≥，即 ASProf1 → ASProf2 意思是 ASProf2 ≥ ASProf1。在图中会发现用于表示 ASProf 之间≥关系的箭头 12、13、16、24、35、47、58、68、79、89。

[0192] 智能卡、PIN、生物统计学的属性和属性值被描绘成与 ASProf 相关联。尤其是，ASProf A4 包括 56 比特智能卡属性 B4，ASProf A7 包括 128 比特智能卡属性 B7，ASProf A6 包括 4 位数 PIN 属性 B6，ASProfA8 包括 10 位数 PIN 属性 B8，以及 ASProf A9 包括包括虹膜辨认属性 B9。在图 1 中也可以有其他属性或属性的结合相关联 ASProf。此外，可以在图 1b 中定义一个指示“没什么安全性 (no securitywhatsoever)”的根节点 ASProf A1 关系到 ASProf 上，例如经由关系 12、13 和 16 联系到 ASProf A2、A3、A6 上。也可以把其他 ASProf 或关系包括到图形中，可以修改或删除已有的 ASProf 或关系。

[0193] 知道有 10 个数目字的 PIN 被定义成≥知道有 4 个数目字的 PIN。用箭头 68 描绘这种≥关系，此箭头 68 始于包括 4 位数 PIN 属性 B6 的 ASProf A6 并指向包括 10 位数 PIN 属性 B8 的 ASProf A8。拥有具有 128 比特密钥的智能卡被定义成≥拥有有 56 比特密钥的智能卡。相应地，用箭头 47 表示 ASProf B7 和 ASProf B4 之间的≥关系，此箭头从 56 比特

智能卡指向 128 比特智能卡。另外，虹膜辨认方法被定义成≥ 10 位数口令以及≥智能卡上的 128 比特密钥，分别用箭头 89 和 79 表示各个≥关系。然而，试着决定是否 10 位数口令≥智能卡上的 128 比特密钥就没多大意义。要是两个 ASProf 之间的≥关系是行不通的或者是不想要的，相应的箭头在图中就不见了。

[0194] 下面给出在图 1b 中描绘的图形 XML 表示的范例。有两个数据结构共同用来代表一个有向图：(a) 使用邻接列表，这是对的列表，每一对代表一个有向边线（有时也叫箭头或关系），对的第一部分规定了各个有向边线的始发 ASProf，第二部分规定了它们的终止 ASProf。(b) 使用关联矩阵 (incidence matrix)，对于每个始发节点都包含一个图中存在的边线所到达的终止节点的列表。在下面的表格 B 中给出的范例中，使用关联矩阵的形式表示。也有可能用其他形式表示。

[0195] <? xml version ＝" 1.0" ? >

[0196] <ASProf_graph>

[0197] <ASProf>

[0198] <name>A1</name> BB1

[0199] <successor>A2<successor>

[0200] <successor>A3<successor>

[0201] <successor>A6<successor>

[0202] </ASProf>

[0203] <ASProf> BB2

[0204] <name>A2</name>

[0205] • • •

[0206] <successor>A4<successor>

[0207] </ASProf>

[0208] <ASProf>

[0209] <name>A3</name>

[0210] • • •

[0211] <successor>A4<successor>

[0212] </ASProf>

[0213] <ASProf>

[0214] <name>A4</name>

[0215] <user_credentials> BB3

[0216] <smart_card>

[0217] <key_length>56</key_length>

[0218] </smart_card>

[0219] </user_credentials>

[0220] <successor>A7<successor>

[0221] </ASProf>

[0222] <ASProf>

[0223] <name>A5</name>

[0224] • • •

[0225] <successor>A8<successor>

[0226] </ASProf>

[0227] <ASProf>

[0228] <name>A6</name>

[0229] <user_credentials> BB4

[0230] <PIN>

[0231] <digits>4</digits>

[0232] </PIN>

[0233] </user_credentials>

[0234] <successor>A8<successor>

[0235] </ASProf>

[0236] <ASProf>

[0237] <name>A7</name> BB5

[0238] <user_credentials>

[0239] <smart_card>

[0240] <key_length>128</key_length>

[0241] </smart_card>

[0242] </user_credentials>

[0243] <successor>A9<successor>

[0244] </ASProf>

[0245] <ASProf>

[0246] <name>A8</name>

[0247] <user_credentials> BB6

[0248] <PIN>

[0249] <digits>10</digits>

[0250] </PIN>

[0251] </user_credentials>

[0252] <successor>A9<successor>

[0253] </ASProf>

[0254] <ASProf>

[0255] <name>A9</name>

[0256] <user_credentials>

[0257] <biometrics> BB7

[0258] <type>iris_scan</type>

[0259] </biometrics>

[0260] </user_credentials>

[0261] </ASProf>

[0262] </ASProf_graph>

[0263] 表 B :利用以 XML 编码的具有图 1b 关系的 ASProf 的范例。

[0264] 表 B 的注释 :

[0265] BB1 :A1 是此图的根节点,它代表空 ASProf 即根本没有安全特征。

[0266] BB2 :在此图中有从根节点 A1 到节点 A2、A3 和 A6 的有向边线。节点的“后继者”被定义为“强度大于或等于”始发节点。

[0267] BB3 :按照图 1b,有属性值“56 比特”的属性 B4 “智能卡”与 ASProfA4 相关。

[0268] BB4 :按照图 1b,有属性值“4 位数”的属性 B6 “PIN”与 ASProfA6 相关。

[0269] BB5 :按照图 1b,有属性值“128 比特”的属性 B7 “智能卡”与 ASProf A7 相关。

[0270] BB6 :按照图 1b,有属性值“10 位数”的属性 B4 “PIN”与 ASProfA8 相关。

[0271] BB7 :按照图 1b,有属性值“虹膜辨认”的属性 B9 “生物统计学”与 ASProf A9 相关。

[0272] ASProf 的属性也可以有分级结构。比如,“密钥长度”属性可能具有不同的解释,这取决于下一较高级属性规定了“TLS 隧道效应”还是“WTLS”。因此,不能总是直接比较“密钥长度”属性的数字值而不首先比较相邻下一较高级属性。

[0273] 在数字属性值的情况下,不需要具有属性值和验证安全强度之间的单调关系,就某种意义来说更大的密钥长度总是意味着更高的验证安全强度。图 2 示出了一个单调关系的范例 :在此范例中,发觉长度大约为 9 的口令的验证安全强度最优。更短的口令被认为较不安全,因为他们更容易被破解,例如在长度非常短的情况下用硬算攻击的方式,对较长的口令用词汇攻击的方式。然而,长于 9 的口令也被认为较不安全,既然它们很难记住所以很可能被用户写下来。属性值“口令长度”和相应的验证安全强度之间的关系在图 2 上部分中示出。下部分示出怎样用有向图的方式表示这个映射,尽管可以想到其他表现方式。有属性口令长度的第一 ASProf 和有属性口令长度的第二 ASProf 之间的关系用相应箭头表示,现在是表示强于 (“>”) 关系的箭头,即用从第二 ASProf 开始到第一 ASProf 上结束的箭头来指示第一 ASProf 强于 (“>”) 第二 ASProf。如果附加的箭头从第一 ASProf 开始到第二 ASProf 上结束,第一 ASProf 和第二 ASProf 就被指示成强度相等 (“=”)。比如,表示两个口令长度的强度相等“=”关系用两个箭头表示,一个箭头从第一口令长度指向第二口令长度,另一个箭头从第二口令长度指向第一口令长度。在这个范例中,有 11-20 个字符的口令被定义成和有 3-6 个字符的口令验证安全强度相等。

[0274] 事实上,完全可以留给服务供应商来决定它的优选和优先属性特征,例如。第一服务供应商为进行单调映射而决定,另一个服务供应商可以按照图 2 的映射来决定映射,以及第三服务供应商可以接受身份供应商默认的图形而不关心映射的细节。

[0275] 图 2 的范例说明了如何用有向图表示非单调关系。它进一步说明了属性值的范围例如“7-10 个字符”,在图示中如何毁坏在单一节点中,即不需要每个被容许的数字值都形成图形中的独立节点。

[0276] 下面,说明由一个或多个身份供应商对于服务供应商 SP 的服务验证用户 :

[0277] 按照图 3,客户机联系服务供应商 SP 提供的服务,用户通过用消息 1a 发送服务请求来调用此服务。服务要求进行用户验证,服务供应商 SP 用消息 1b 向客户机发送进行用户验证的请求。客户机用消息 1c 把用户身份提供给服务供应商 SP,服务供应商 SP 可以检验用户身份。如果用来验证客户机的身份供应商 IdP1 是服务供应商 SP 未知的,客户机就

用消息 1c 向 SP 发送一个身份供应商 IdP1 的参考，例如统一资源标识符 (URI)。可选择地，从客户机默认地向服务供应商 SP 发送身份供应商 IdP1 的参考。

[0278] 服务供应商 SP 通过用消息 2 向身份供应商 IdP1 发送期望的 ASProf 和用户身份来请求验证用户，此 ASProf 规定了服务的验证安全要求。典型地，服务供应商 SP 和身份供应商 IdP1 正在建立安全会话（例如使用 TLS），该会话为他们交换的信息提供了机密性、完整性和可靠性，以及服务供应商 SP 和身份供应商 IdP1 之间单向或双向的验证。对于推荐的验证方法中所涉及的任何类型的实体之间任何类型的加密所必需的处理和消息既没有在图 3 中也没有在后面的图形中描绘。

[0279] 身份供应商 IdP1 在处理 3a 中检查它是否可以满足从 SP 接收的 ASProf 中所述的要求。如果可以满足要求，身份供应商 IdP1 可以在处理 3a 中进一步检查是否需要检验用户凭证。如果凭证检验是必需的，就向客户机发送对用户凭证的请求 3b，而客户机可以通过提供所请求的用户凭证从而用消息 3c 响应这个请求 3b。对于请求 3b 和相应的响应 3c 来说频带内和频带外通信都有可能。基于检查 ASProf 的要求和任选的凭证检验得到的正向结果，身份供应商 IdP1 用消息 3d 向 SP 发送进行用户检验的断言。基于此断言，服务供应商 SP 可以准许对客户机进行访问，以访问被请求服务的会话。

[0280] 作为检验用户凭证的范例：用户已经在上午 9 点使用用户名 / 口令机制经由一个 IdP 验证到自己收藏的 web 门户。在上午 11 点，用户想访问在提供互联网图书销售服务的服务供应商上他的简档，而所述服务供应商还接受来自同一 IdP 的验证断言。如果所述服务供应商在它 ASProf 中要求口令输入不能超过一个小时，IdP 就需要在用户被验证到所述服务供应商上以前请求用户再次输入口令。另一方面，如果所述服务供应商接受高达 24 小时陈旧的口令输入，就没必要再次输入口令了。

[0281] 按照图 3 和图 3 上的说明，只有一个 ASProf 从服务供应商 SP 向身份供应商 IdP1 发送。然而，把推荐的方法用于这样的情况也容易，即多个期望的 ASProf 从服务供应商 SP 向身份供应商 IdP1 发送。在这种情况下，服务供应商 SP 发送 ASProf 的“希望列表”，也就是服务供应商 SP 认为可以充分验证用户的 ASProf。身份供应商 IdP1 检查希望列表。如果希望列表上的一个或多个 ASProf 是身份供应商 IdP1 所支持的，身份供应商 IdP1 可以选择 ASProf 中他最佳支持的那一个，例如不需凭证检验或者凭证检验与希望列表中其他被支持的 ASProf 相比没有那么困难。

[0282] 结合图 3 说明的方法是使用“反信道”消息流，涉及身份供应商 IdP1 和 SP 之间直接进行的消息交换。换句话说，也可以使用“前信道”来实施此方法，即身份供应商 IdP1 和服务供应商 SP 之间的任何通信都由客户机中继，最好使用合适的安全性预防措施，以使客户机不能窜改往返通过的信息。对于不同消息反信道和正信道的结合也有可能。

[0283] 对于为了完成图 3 的验证而进行的前信道通信的范例在图 4 中描绘。在前信道通信中，用消息 42a 从服务供应商 SP 向客户机发送期望的 ASProf 和选择地发送用户身份。客户机用消息 42b 向身份供应商 IdP1 发送期望的 ASProf 和用户身份。如果用户身份不由服务供应商 SP 提供，则客户机获取用户身份并用消息 42b 把它发送给身份供应商 IdP1。如图 3 中所示，身份供应商 IdP1 可以在处理 3a 中检查接收的 ASProf 以及是否必须进行凭证检验。如果是这样，身份供应商 IdP1 可以使用消息 3b、3c 来检验用户凭证。如图 3 中所示，消息 3b、3c 是可选择的，并且可以利用带内或带外通信。用消息 43d、43e 经客户机向服务

供应商 SP 发送由身份供应商 IdP1 给出的安全断言。在这种情况下，安全断言被认为是验证令牌或者记录单 (ticket)。

[0284] 在移动客户机的情况下，反信道实施方案有利于避免服务供应商 SP 和身份供应商 IdP1 之间越过客户机的空中接口进行通信。对于前信道通信，唯独为了在服务供应商 SP 和身份供应商 IdP1 之间往返传递信息就在空中接口上使用了额外的带宽并导致额外的等待时间。

[0285] 前信道解决方案是像互联网这样的固定网常用的，与反信道解决方案相比它更好地减少了执行难度。它还有发生会话重定向的优点，即图 4 的 1c 中向服务供应商 SP 的请求由消息 42a 中来自服务供应商 SP 的答复来回应，而不像在反信道情况下由来自身份供应商 IdP1 的答复来回应。这可能导致验证所需的全部时间比反信道通信更短了。

[0286] 混合执行方案也有可能，例如使用代理服务器，从而赶超用于在服务供应商 SP 和身份供应商 IdP1 之间通信的前信道，同时避免了流过客户机的业务量。因而混合执行方案对于移动客户机来说非常有用。

[0287] 对于这个情况，结合图 3 所述的身份供应商 IdP1 不支持从服务供应商 SP 向身份供应商 IdP1 发送的期望的一个或多个 ASProf，身份供应商 IdP1 把对一个或多个期望的 ASProf 的反建议提供给服务供应商 SP。按照图 5，服务供应商 SP 用消息 2a 向身份供应商 IdP1 发送包括期望的 ASProf 和用户身份的验证请求。身份供应商 IdP1 检查收到的期望的 ASProf 并认识到期望的 ASProf 不被支持。一个或多个可选择的 ASProf 被确定并作为推荐的可选择的 ASProf 被用消息 4a 从身份供应商 IdP1 向 SP 发送。服务供应商 SP 在处理 5a 中检查是否一个或多个推荐的可选择的 ASProf 之中至少有一个可以接受。如果接收的推荐的可选择的 ASProf 之中没有一个可以接受，服务供应商 SP 就可以向用来进行检验的身份供应商 IdP1 发送一个或多个其它期望的 ASProf，或可以和其他用来进行检验的身份供应商 IdP1 取得联系或者终止此验证。如果一个或多个推荐的可选择的 ASProf 之中至少有一个可以接受，服务供应商 SP 就用消息 5b 向身份供应商 IdP1 发送对至少一个推荐的可选择的 ASProf 的批准。如果多个推荐的可选择的 ASProf 都可以接受，服务供应商 SP 就选择多个 ASProf 之一，之后发送对选取的 ASProf 的批准，例如服务供应商 SP 可以检查收到的一个或多个推荐的可选择的 ASProf 并在发现第一个 ASProf 可以接受以后停止检查。这个 ASProf 由服务供应商 SP 批准并且把批准这个 ASProf 的指示发送给身份供应商 IdP1。对于批准了的 ASProf，身份供应商 IdP1 用结合图 3 所述的处理和消息 3a-3d 继续进行处理。

[0288] 如上面结合图 3-5 所述，服务供应商 SP 想要身份供应商 IdP1 使用一个或多个 ASProf 意味着把期望的一个或多个 ASProf 发送给身份供应商 IdP1。然而，服务供应商 SP 不必向身份供应商 IdP1 发送一个或多个期望的 ASProf 来请求验证。取而代之，服务供应商 SP 可以请求从身份供应商 IdP1 发送一个所支持的 ASProf 的列表。这在图 6 中示出。服务供应商 SP 用消息 62a 向身份供应商 IdP1 发送用户身份并请求验证。身份供应商 IdP1 用带有身份供应商 IdP1 所支持的 ASProf 的列表的消息 62b 来响应。服务供应商 SP 在处理 62c 中检查此列表并从列表中选择一个可以接受的 ASProf。用消息 62d 向身份供应商 IdP1 发送选取的 ASProf（作为指示的一个示范）或选取的 ASProf 的指示。发送选取的 ASProf（作为指示的一个示范）或指示可以再补充以用户身份，用于使选取的 ASProf 与用消息 62a 发送的验证请求相关联。身份供应商 IdP1 可以在处理 63a 中检查对选取的 ASProf 来说是否

有必要进行凭证检验，用结合图 3 所述的处理和消息 3a-3d 来继续处理。

[0289] 通过发送各个具有或不具有体现安全强度等级的关系的 ASProf 可以完成 ASProf 的发送。可以发送各个 ASProf 或者 ASProf 和关于 ASProf 之间关系的信息。比如，就结合图 1 和 2 所述的图形表示法来说，可以发送整个图形和图形的各个部分，像 ASProf 和箭头。ASProf 的发送者例如服务供应商 SP 可以规定哪些 ASProf 是想要接收者使用的，例如身份供应商 IdP1。特别地，如果接收者不支持期望 ASProf 中的任何一个，接收者可以在图形上从期望的 ASProf 开始导航以查看是否他能支持一个 ASProf，这一个 ASProf 被认可为强度大于或等于期望的 ASProf，如果关于 ASProf 之间关系的信息是接收者可以得到的。当导航通过接收者已知的图形或图形的各个部分时，接收者可以选择至少一个强度大于或等于的 ASProf，以满足发送者期望的 ASProf 的强度上的要求。

[0290] 对于导航的相应示范在图 7 中描述，其中服务供应商 SP 用消息 72 向用来进行验证的身份供应商 IdP1 发送整个 ASProf 图形或其中一部分、对期望的 ASProf 的指示和用户身份。不发送整个图形，服务供应商 SP 能够只发送图形中包括强度大于或等于期望的 ASProf 的 ASProf 的那部分，例如从而降低发送努力或者从而不给身份供应商 IdP1 提供这个验证不可用的信息。身份供应商 IdP1 在处理 73a 中检查期望的 ASProf 是否被支持。如果它不被支持，身份供应商 IdP1 在处理 73a 中通过导航搜索从 SP 接收的图形来检查是否有更强的 ASProf（如图 7 中所绘）或强度相等的 ASProf 被支持。如果强度大于或等于而且与不被支持的期望的 ASProf 不同的至少一个 ASProf 是身份供应商 IdP1 所支持的，身份供应商 IdP1 就如结合图 3 所述（处理和消息 3a-3c）那样在处理 73a 中检查检验用户凭证并请求用户发送它们是否必要。如果使用一个等强度或更强的 ASProf 并可选择地检验用户凭证，身份供应商 IdP1 就用消息 73d 向身份供应商 IdP1 发送一个进行用户验证的断言，其最好再补充上对所用的等强或更强的 ASProf 的指示。在允许客户机进行服务访问以前，服务供应商 SP 可以在处理 73e 中检查所用的 ASProf 是否是服务供应商 SP 可以接受的，例如是否遵照服务供应商 SP 的验证安全要求。

[0291] 如上面所解释发送此图形或此图形的某些部分使推荐的方法在消息往返传播数量上更加有效，如果服务供应商 SP 和身份供应商 IdP1 共同分享至少在某种程度上相似的想法，这使 ASProf 强度大于或等于另一个 ASProf，即他们共同分享关于 ASProf 和 ASProf 之间相对于验证安全强度上的关系的信息。此外，发送此图形有利于使服务供应商 SP 和身份供应商之间的消息往返传播数量最小，从而使验证服务快多了，同时还保证 SP 安全优选和优先级被察觉。

[0292] 比如，如果服务供应商 SP 请求一个 128 比特的密钥长度，而身份供应商只能提供或 64 比特或 256 比特，那么服务供应商 SP 和身份供应商共同拥有这样一个观念，即 256 比特密钥比 128 比特密钥更强被服务供应商 SP 接受了。如果不是共同拥有这个观念，那么需要交换附加的消息直到服务供应商 SP 和身份供应商同意采用某个 ASProf。如果不知道 256 比特密钥比 128 比特密钥更强这个关系，身份供应商就发送比如 128 比特密钥不被支持的一个指示给服务供应商 SP。对于这种情况，服务供应商 SP 可以用被支持的 256 比特的可选择 ASProf 来响应。

[0293] 一个 ASProf 强度是否大于或等于另一个 ASProf 这个共同拥有的观念可能是明显的也可能是隐含的。对隐含认同的示范是上面 128 比特对 256 比特的情况，意味着 256 比

特通常可以理解为强于 128 比特。假设服务供应商 SP 在请求了 128 比特的时候发现 256 比特可以接受，不能提供 128 比特的身份供应商就用 256 比特代替并在 ASProf 中把这件事告知服务供应商 SP。然而，如果服务供应商 SP 用了与身份供应商不同的 ASProf 强度的定义，身份供应商错误的假设导致附加的再次协商和附加的消息或者验证终止。一个示范是服务供应商 SP 和身份供应商之间共同拥有的明显观念与图 2 中给出的共同拥有的隐含观念相比更优选，在图 2 服务供应商 SP 定义了一个数字属性和被发觉的验证安全强度之间非单调的不被普遍认同的关系。

[0294] 图 8 示出了一个验证，服务供应商 SP 用消息 2 发送一个包括期望的 ASProf 和用户身份的验证请求，但不发送其他关于 SP 的图形的信息。如处理 83a 中所示，身份供应商 IdP1 不支持期望的 ASProf，并且它挑选一个可选择的 ASProf。身份供应商在处理 83a 中检查是否有必要进行凭证检验。按照结合图 3 所给出的解释使用消息 3b 和 3c 来可选择验证用户凭证之后，用消息 83d 向 SP 发送进行用户验证的断言和所用的可选择的 ASProf 的指示给 SP。服务供应商 SP 在处理 83e 中检查可选择的 ASProf 是否可以接受。如果此 ASProf 可以接受，就开始服务会话。为了挑选可选择的 ASProf，ASProf 可以使用它自己的表示法，例如通过使用自己的图形或假定的明显的表示法。然而，为了避免服务供应商 SP 发现可选择的 ASProf 不可接受，身份供应商 IdP1 最好使用服务供应商 SP 和身份供应商 IdP1 之间共同使用的表示法。在对于身份供应商 IdP1 所提供的验证服务注册服务供应商 SP 时可以提供反映根据服务供应商 SP 的顺序的图形。然而，对于特别情形除了期望的 ASProf 和用户身份没有其他信息是身份供应商 IdP1 可以得到的，身份供应商 IdP1 最好可以使用它自己的表示法，例如他自己的图形，或可以向身份供应商请求一个或多个被支持的 ASProf，例如以图形的形式。

[0295] 通过用关系把 ASProf 联系起来，可以创建几组 ASProf。比如，通过用＝关系把所述数量的 ASProf 中的每一对联系起来从而形成一组有相等验证安全强度的 ASProf，很多个 ASProf 被联系起来，例如如图 2 中所指示由具有 3-6 和 11-20 个字符的 ASProf 形成相等验证安全强度的一组。服务供应商可以通过从属于用来验证用户的某个组的 ASProf 之中选择一个来向身份供应商指示要使用属于这组的 ASProf 中的任何一个并向身份供应商发送选取的 ASProf 的指示，用来验证用户。如果身份供应商察觉到了指示的组，例如由于下述事实，由服务供应商 SP 向 IdP 或由后者向前者提供关于此组的特性的信息，即 ASProf 和他们的关系，身份供应商就可以基于指示从此组之中选择某个 ASProf 用来进行验证。如果服务供应商和身份供应商共同使用此组的同一个表示法，就可以使用一个组标识符向身份供应商指示此组。可以把各个组分级排序，例如把包括第一数目个 ASProf 的第一组相关联到第二组 ASProf，并且身份供应商可以从一组导航搜索到另一组。为了检查执行验证所基于的那个 ASProf 是否与服务供应商的验证安全强度相匹配，所述验证安全简档所关联的组的指示可能是充分的。形成组的优点在于带有可比的特性的验证安全简档有了更好的可定标性和可管理性，其中可比的特性像可比的凭证类型、可比的创建或有效期。

[0296] 作为另一种验证方法，服务供应商 SP 可以请求验证而不规定任何 ASProf。在图 9 中描述了相应情形。服务供应商 SP 用消息 62a 向身份供应商 IdP1 发送一个包括用户身份的验证请求。身份供应商 IdP1 如处理 93a 中所指示那样使用它自己选择的 ASProf，并且可选择地通过例如利用结合图 3 所解释的消息 3b、3c 来按照选取的 ASProf 执行凭证检验。

然后，身份供应商 IdP1 用消息 93d 把所用的 ASProf 的指示或者所用的 ASProf 本身作为另一种形式的指示与验证的断言一起向服务供应商 SP 发送。然后服务供应商 SP 决定是否接受此验证，即在处理 93e 中检查所用的 ASProf 是否可以接受。

[0297] 在下面两图 10 和 11 中说明了用来在服务会话期间由身份供应商向服务供应商 SP 更新用户验证的方法。按照图 10，一个客户机参与服务会话。在利用对于服务供应商的服务第一次用户验证建立服务会话可以按照图 3 到 9 的说明来完成。在服务会话期间，客户机访问一个服务，此服务要求一个比已建立的会话更高的安全等级。对更高的安全等级的示范是可以通过 5 位数 PIN 码访问他在线银行账户的用户。然而，如果用户又想从他的银行账户授权一笔现金交易，就需要另外一个一次口令或者 TAN。另一个示范，用户可以通过口令访问他个人化的 web 门户。门户上的一些服务往往是收费的。当用户在这样一个服务上点击时，需要使用连接到用户 PC 上的智能卡读出器进行验证。

[0298] 服务供应商 SP 检测用消息 102a 从客户机向服务供应商 SP 发送的服务请求并选择一个 ASProf，下文中被称为修正的 ASProf，它满足更严格的要求，即修正的 ASProf 比第一次验证所用的 ASProf 更强。服务供应商 SP 用消息 102b 向身份供应商发送一个包括修正的 ASProf 和用户身份的验证请求并选择 ASProf，此身份供应商不必与第一次验证所用的身份供应商相同。身份供应商 IdP1 在处理 103a 中检查它是否能够满足更强的 ASProf 要求。如果它能满足，身份供应商 IdP1 在处理 103a 中检查这个更强的 ASProf 是否需要重新检验用户凭证并且如果需要就用消息 103b、103c 完成这个检验。如图 3 中所示，可选择消息 103b、103c 可以用带内或频外通信交换这两个消息。然后如结合图 3 所述对于用消息 103d 从身份供应商 IdP1 向服务供应商 SP 发送的进行用户验证的断言继续进行处理。基于此断言，服务供应商 SP 可以允许访问要求升级 ASProf 的服务并且服务会话能够继续进行。不发送选取的 ASProf（作为指示的一种形式），而发送对选取的 ASProf 的指示像 URI，例如当选取的 ASProf 是身份供应商 IdP1 已知的或者可访问的。如果第一次验证中所用的 ASProf 是身份供应商 IdP1 已知的，服务供应商 SP 就发送一个指示以便使用比第一次验证中所用的 ASProf 更强的 ASProf。在这种情况下，身份供应商 IdP1 可以例如通过导航图形来执行对修正的 ASProf 的选择。最好，这个被用来升级验证的修正的 ASProf 被指示给服务供应商 SP 并被它批准用来升级验证。

[0299] 图 11 示出由第一身份供应商 IdP1 建立起验证和服务会话并且客户机请求对要求更高安全等级的服务进行服务访问。服务供应商 SP 因而检测要求更高安全等级的用消息 102a 发送的服务请求并用消息 102b 向第一 IdP 发送包括修正的 ASProf 和用户身份的验证请求。第一身份供应商 IdP1 在处理 113a1 中检查收到的修正的 ASProf 并检测到修正的 ASProf 不被支持。因此，第一身份供应商 IdP1 用消息 113b 发送对修正的 ASProf 的拒绝和可选择的对第一身份供应商 IdP1 推荐的可选择的 ASProf 的拒绝。服务供应商 SP 可以在处理 113c 中检查可选择的 ASProf 并且会发现它们是不可接受的。可以把对此拒绝的响应发送给第一身份供应商 IdP1 来指示验证对于第一身份供应商 IdP1 来说被终止了。在这一点上，服务供应商 SP 可以使验证升级终止或者可以挑选第二身份供应商 IdP2 用来进行验证升级。如果有第二身份供应商 IdP2 可以用，就用消息 112b 向第二身份供应商 IdP2 发送另一个验证请求。另一个请求包括修正的 ASProf 和用户身份，后者可以与在第一身份供应商 IdP1 上用于第一次验证的用户身份完全相同或不同。第二身份供应商 IdP2 在处理

113a2 中检查修正的 ASProf 是否被支持。如果修正的 ASProf 不被支持，需要的话，例如通过利用带内或频外通信的消息 113b、113c 来执行用户凭证的检验。用消息 113d 向 SP 发送用户验证的断言。基于这个断言，服务供应商 SP 可以批准访问有更严格安全要求的服务，并且服务会话可以继续进行。

[0300] 另一个示范性的升级情形是：用户由他的互联网服务供应商（ISP）有时也叫互联网接入供应商通过口令进行验证。在时间的某一刻上，用户想访问视频流服务，此服务往往是收费的而且要求更强的验证，例如用移动电话（用户身份模块/无线标识模块，SIM/WIM）作为验证令牌。服务供应商，即视频服务流服务的供应商，首先联系用来验证升级的 ISP。ISP 因为它一般不管理 SIM 和移动电话，可能只有简单口令列表不能满足更严格的 ASProf。它可以向服务供应商推荐一个更弱的 ASProf，但服务供应商拒绝。服务供应商然后联系用户的移动操作员，它是由客户机在初始的服务请求中规定为潜在的身份供应商的。作为身份供应商的移动操作员能够满足规定的 ASProf，即要求拥有特定的 SIM/WIM 以及知道 PIN 代码。它发送更强的验证的断言给服务供应商，从而用户可以继续使用此流式服务。

[0301] 无论何时从身份供应商向服务供应商发送 ASProf，不必要每次都明显地全部写出 ASProf 的整套属性，反之亦然。相应地，不必完全发送 ASProf 之间的关系或全部图形。取而代之，为了减少交换的数据量可以使用参考（URI）以及更新，如下面所解释的。

[0302] 一个 ASProf 可以由一系列片断（fragment）组成，每个都规定一个或多个属性，例如按照表 A 的 XML 描述与涉及 <user_credentials>、<transport_layer_security>、<security_policies> 和 <user_registration> 的片断作比较。来自各个片断的属性或者互相补充，即如果它们只在一个片断中出现或者互相覆盖，即如果它们在两个片断中都出现。在覆盖的情况下，需要基于片段的排序规定优先权法则，即后续片断覆盖先前的，或者相反。

[0303] 参考例如最好是 URI，可以被用来指向 ASProf 或指向片断，片断最好代表全部 ASProf 的语义子集，代替明显地全部拼写这个 ASProf 或片段的所有属性。使用参考使得提取数据和缓冲存储成为可能而且可以基本上减少往返发送的数据量。例如，当服务供应商频繁使用某个身份供应商时，该身份供应商在某个时间段使用同一个 ASProf，不需要每次在所述的某个时间段内验证新用户的时候都在服务供应商和身份供应商之间明显地交换 ASProf。

[0304] ASProf 更新的使用可以进一步减少交换的数据量，意味着与已有的 ASProf 和较新的 ASProf 之间的差有关的 Δ（delta）更新。更新 ASProf 是或者补充已有的 ASProf 或者覆盖其一些属性的较新的 ASProf。还可能有更新片断或更新属性。比如，身份供应商使用口令检验对于服务供应商进行用户验证。对于某个用户交互，需要验证更新，其中与先前用的 ASProf 的唯一区别是给对于口令检验规定了更短的有效时间（time-to-live）。在这种情况下，相对于发送接收部件得完全提取和缓冲存储的新 ASProf 的参考，显然把参考发送给先前用的 ASProf 就有效得多，加上规定偏离有效时间属性的单一属性。

[0305] 推荐的方法还体现在与服务供应商、身份供应商或者代理或客户设备相关的设备中，像服务器。这种设备包括用来接收消息 M2 的至少一个接收单元 R、用来发送消息 M1 的发射单元和用来处理消息和信息的处理单元 P，并且最好包括用于存储信息的数据库 D。在图 12 中描绘了这种设备的范例，图中示出单元 R、T、P、D 和消息 M1、M2 和用来在各个单元

R、T、P、D 之间交换信息和消息的互连 PR、PT、PD。设备 DEV 是服务供应商、身份供应商或者像客户设备这样的用户可以采用来实施此方法的设备的一个范例。

[0306] 在用来执行验证方法的设备之间交换消息和信息的设备和链路在图 13、14 和 15 中分别对反信道、前信道和反 / 前混合信道通信给出范例。可以结合图 12 所绘所述构成这些设备。

[0307] 图 13 示出客户机 D12、服务供应商 D10 和身份供应商 D11 以及这三者之间的链路 CON10、CON11、CON12，用来经由前信道通信对于服务供应商 D10 验证客户机 D12。经由链路 CON10 来进行客户机 D12 和服务供应商 D10 之间的通信，经由链路 CON11 来进行服务供应商 D10 和身份供应商 D11 之间的通信，经由链路 CON12 来进行身份供应商 D11 和客户机 D12 之间的通信。经由链路 CON10、CON11、CON12 在这三者之间交换信息和消息的范例在例如图 3 中可以找到，即经由链路 CON10 的服务请求（消息 1a）、验证请求（消息 1b）、用户身份和身份供应商参考（消息 1c）以及服务会话，经由链路 CON11 的期望的 ASProf 和用户身份（消息 2）以及用户验证的断言（消息 3d），还有经由链路 CON12 的用户凭证请求（消息 3d）和用户凭证递送（消息 3d）。链路 CON10、CON11、CON12 可以但不必是固定连接，例如如果客户机 D12 是一部移动电话，就可以经由短消息业务 (SMS) 获得链路 CON12。

[0308] 图 14 示出客户机 D22、服务供应商 D20 和身份供应商 D21 以及这三者之间的链路 CON20、CON21，用来经由前信道通信把客户 D22 验证到服务供应商 D20。对照图 11，服务供应商 D20 和身份供应商 D21 之间不存在直接链路。取而代之，经由客户机 D22 在服务供应商 D20 和身份供应商 D21 之间实现通信。服务供应商 D20 和身份供应商 D21 之间交换的信息被客户机 D22 中继。经由链路 CON20 和 CON21 在这三者之间交换信息和消息的范例在例如图 4 中可以找到，即经由链路 CON20 发送服务请求（消息 1a）、验证请求（消息 1b）、用户身份和身份供应商参考（消息 1c）以及服务会话。相应地，经由链路 CON21 发送用户凭证请求（消息 3b）和用户凭证。然而，期望的 ASProf 和包含在验证请求中的用户身份（消息 42a、42b）经由链路 CON20 和 CON21 从服务供应商 D20 经由客户机 D22 向身份供应商 D21 发送。为了经由链路 CON20 和 CON21 从身份供应商 D21 经由客户机 D22 向服务供应商 D20 发送的用户验证的断言（消息 43d、43e）而实现相应的中继。

[0309] 图 15 示出混合实现使用代理 D31 来赶超前信道实现。为了把客户机 D33 的用户验证到服务供应商 D30 的服务，客户机 D33 经由链路 CON30 向服务供应商 D30 发送服务请求。服务供应商 D30 经由链路 C30 用用户验证请求来响应客户机，客户机 D33 把用户身份和选择地将身份供应商 D32 的参考经由链路 CON30 提供给身份供应商 D32。为了在服务供应商 D30 和身份供应商 D32 之间进行通信，例如为了发送用户身份和期望的 ASProf 或者为了用户验证的断言，把代理 D31 置于在服务供应商 D30 和身份供应商 D32 之间。从服务供应商 D30 到身份供应商 D32 的信息和反过来的信息可以使用连接 CON31 和 CON32 经由代理 D31 来发送。对于用户凭证请求和用户凭证的递送，可以使用链路 CON35。选择地，链路 CON34 和链路 CON34 能够用于用户凭证的请求和传送。在代理 D31 和客户机 D33 之间经由链路 CON34 可以交换其他信息。

[0310] 按照此发明的方法还体现在一个或多个计算机程序，这些计算机程序可装载到与服务供应商、身份供应商、代理或客户机相关的设备中。一个或多个计算机程序包括软件代码部分，以便实施上述方法。可以把一个或多个计算机程序存储在计算机可读媒体上。计

算机可读媒体可以是服务器内部或外部的或者放在外面的永久性或可再写性存储器。还可以把计算机程序服务器例如作为信号序列经由电缆或无线链路转移到服务器。

[0311] 推荐的方法适合用在像 GPRS 这样的 2G 和像 UMTS 这样的 3G 移动电信系统中。还可以应用于对像互联网这样的固定网络以及固定网络和无线网络的结合中的服务进行验证，无线网络包括无线局域网 (WLAN)。用户可以采用移动和固定客户机终端。与服务供应商、身份供应商或代理相关的服务器一般在网络中是固定的。然而，可以把推荐的方法应用到运动着的非固定的客户机上。服务器的范例是个人计算机 (PC) 或膝上型电脑。

[0312] 下面，对本发明优点的其中一些进行总结：

[0313] 对于稳态验证安全策略在服务供应商和身份供应商之间不具有固定关系，此发明能够提供验证安全简档的特殊协商和升级。对于特殊协商，不需要关于 ASProf 的服务供应商和身份供应商之间任何在先协议。

[0314] 而且，不同类型的服务和可能对于知道用户是他所宣称的那个人的确定性有非常不同的要求。同样地，不同的验证机制和安全基础结构提供了不同等级的确定性。推荐的方法支持这些不同等级的确定性，从而克服二元验证概念都有的限制。

[0315] 另一优点是本发明提供了灵活模型，允许在服务供应商一方和在身份供应商一方的策略在传输过程中改变。如果策略和安全性特征改变，就可以最小化服务供应商和身份供应商之间的带外通信。

[0316] 而且，此验证方法允许管理 ASProf 的复杂规定，即不同类型的属性像指纹辨别和口令可以相对于验证安全强度进行比较。而且，也可以协商不同属性的结合，以使此推荐的方法更通用。

[0317] 还有，此验证方法使各个服务的服务供应商有权充当最终做出关于验证的决定的策略决定和策略强制点。对于这个服务供应商友好的情况，能够实施推荐的发明，从而身份供应商提供确认用户凭证的服务而且身份供应商最好只参与会话建立或者只用于验证更新。在会话期间对身份供应商没有别的要求，由此减少了身份供应商的负载及其会话管理的复杂性，并且与现有技术的具有中间身份供应商的验证方法相比改善了可缩放性。

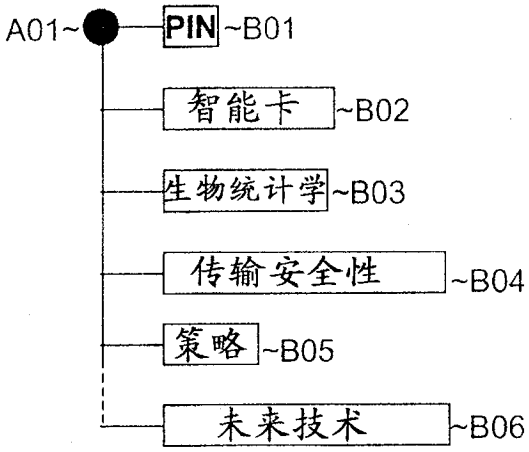

A01~
PIN ~B01
智能卡 ~B02
生物统计学 ~B03
传输安全性 ~B04
策略 ~B05
未来技术 ~B06

图 1a

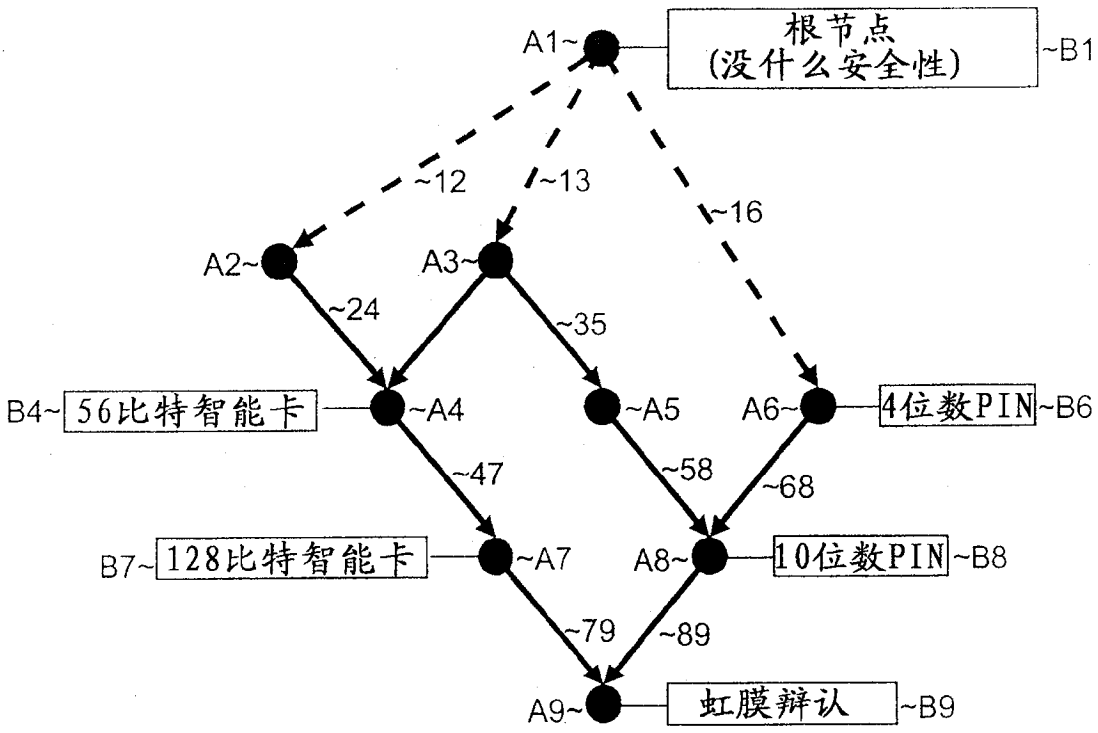
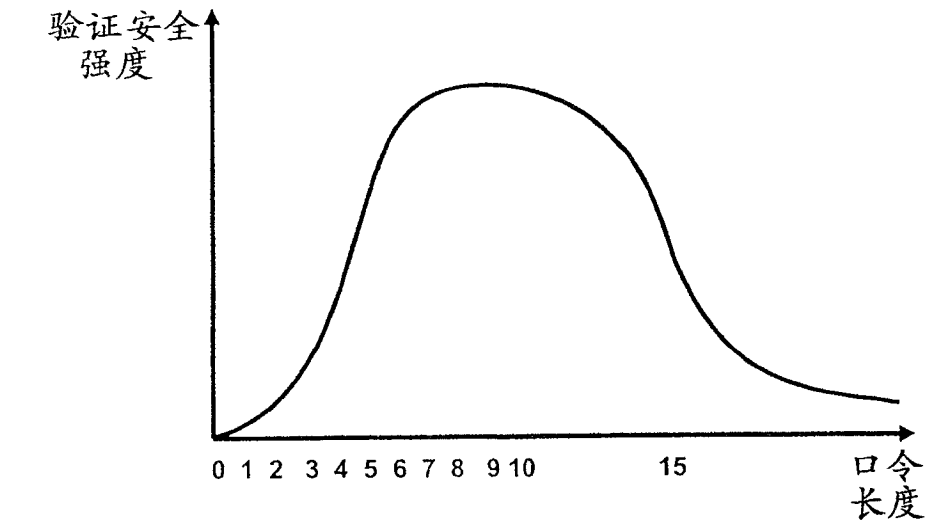

A1~
根节点
(没什么安全性)
~B1
~12
~13
~16
A2~
A3~
~24
~35
B4~
56比特智能卡
~A4
~A5
A6~
4位数PIN ~B6
~47
~58
~68
B7~
128比特智能卡
~A7
A8~
10位数PIN ~B8
~79
~89
A9~
虹膜辨认 ~B9

图 1b


验证安全强度
0 1 2 3 4 5 6 7 8 9 10
15
口令长度

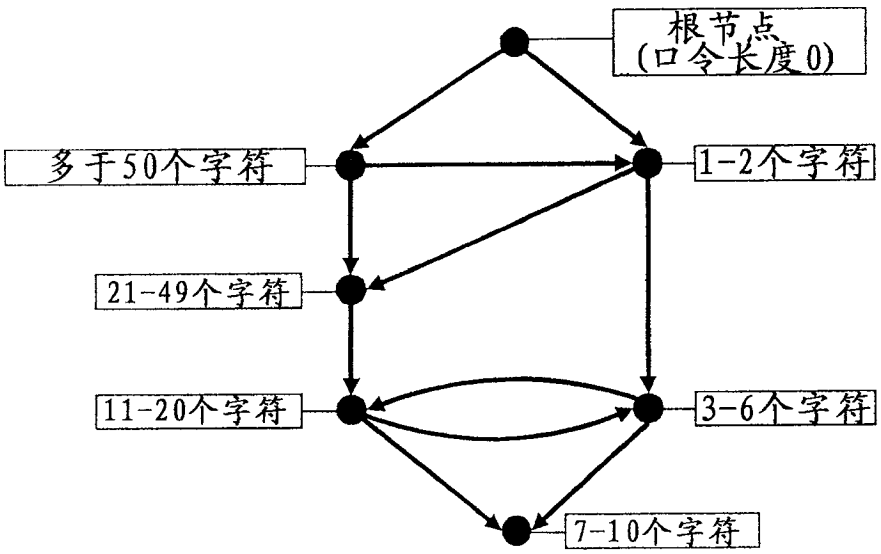

根节点
(口令长度0)
多于50个字符
1-2个字符
21-49个字符
11-20个字符
3-6个字符
7-10个字符

图 2

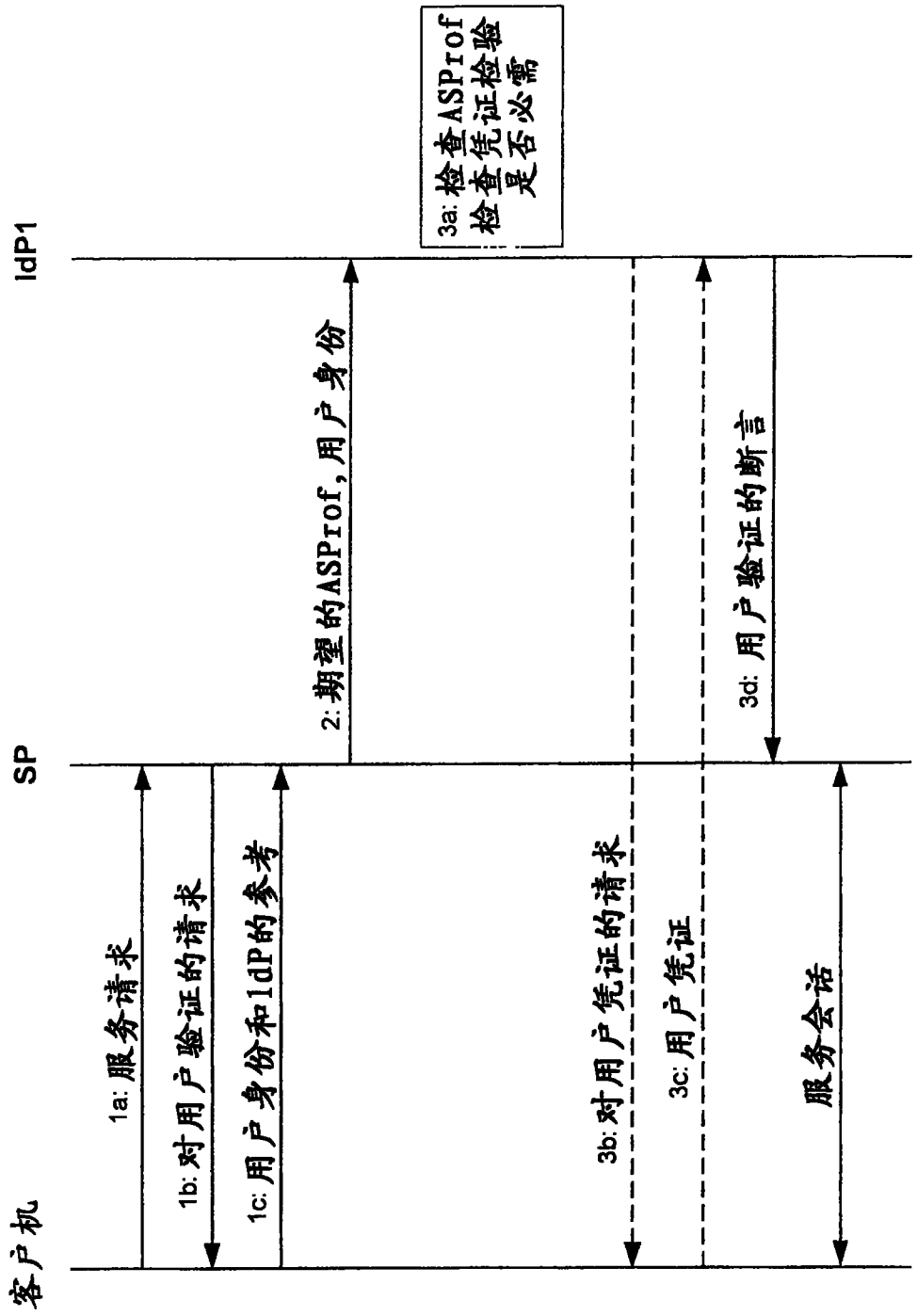

客户机
SP
IdP1
1a: 服务请求
1b: 对用户验证的请求
1c: 用户身份和IdP的参考
2: 期望的ASProf，用户身份
3a: 检查ASProf
检查凭证检验
是否必需
3b: 对用户凭证的请求
3c: 用户凭证
3d: 用户验证的断言
服务会话

图 3

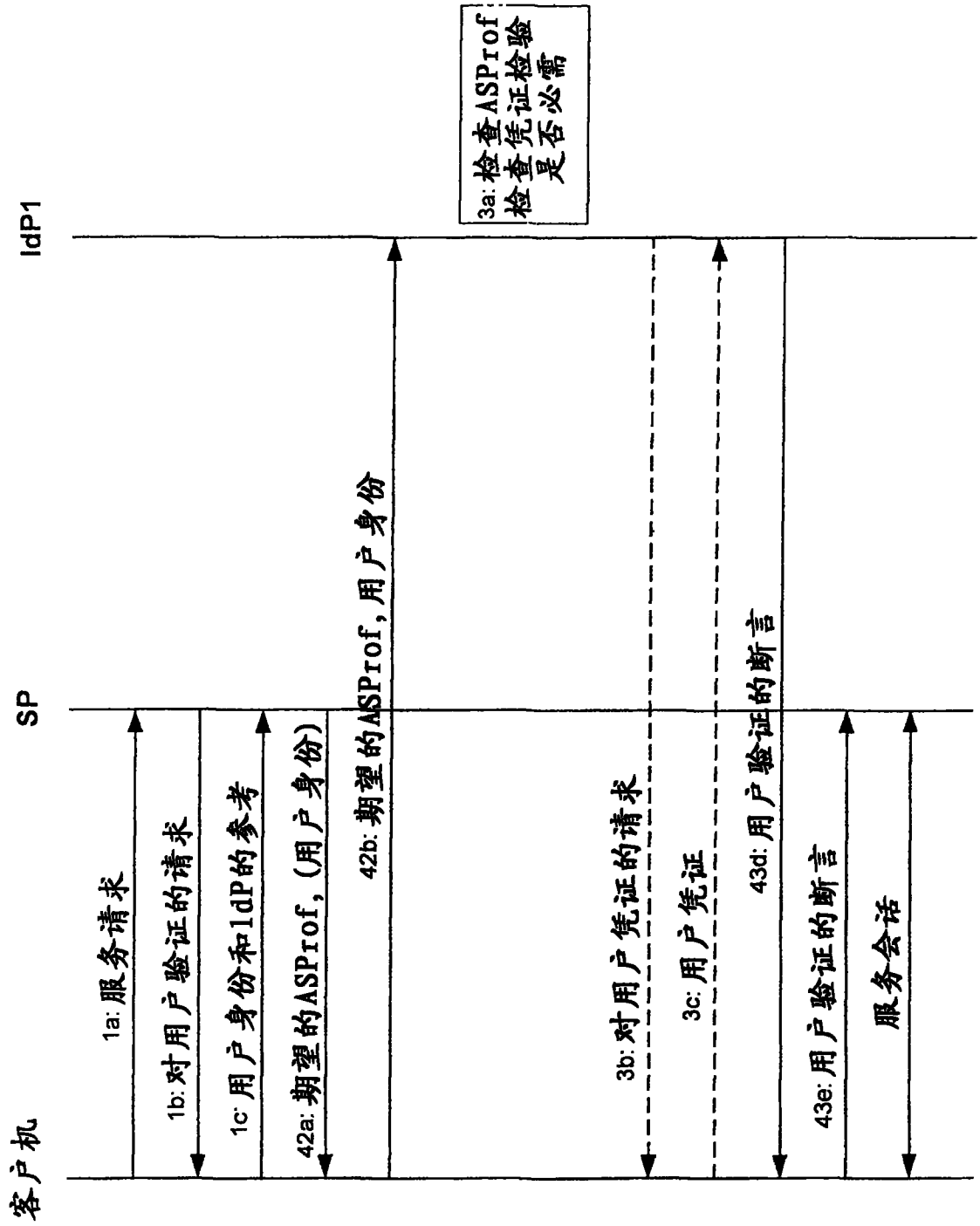

客户机
SP
IdP1
1a: 服务请求
1b: 对用户验证的请求
1c: 用户身份和IdP的参考
42a: 期望的ASProf，(用户身份)
42b: 期望的ASProf，用户身份
3a: 检查ASProf检查凭证检验是否必需
3b: 对用户凭证的请求
3c: 用户凭证
43d: 用户验证的断言
43e: 用户验证的断言
服务会话

图 4

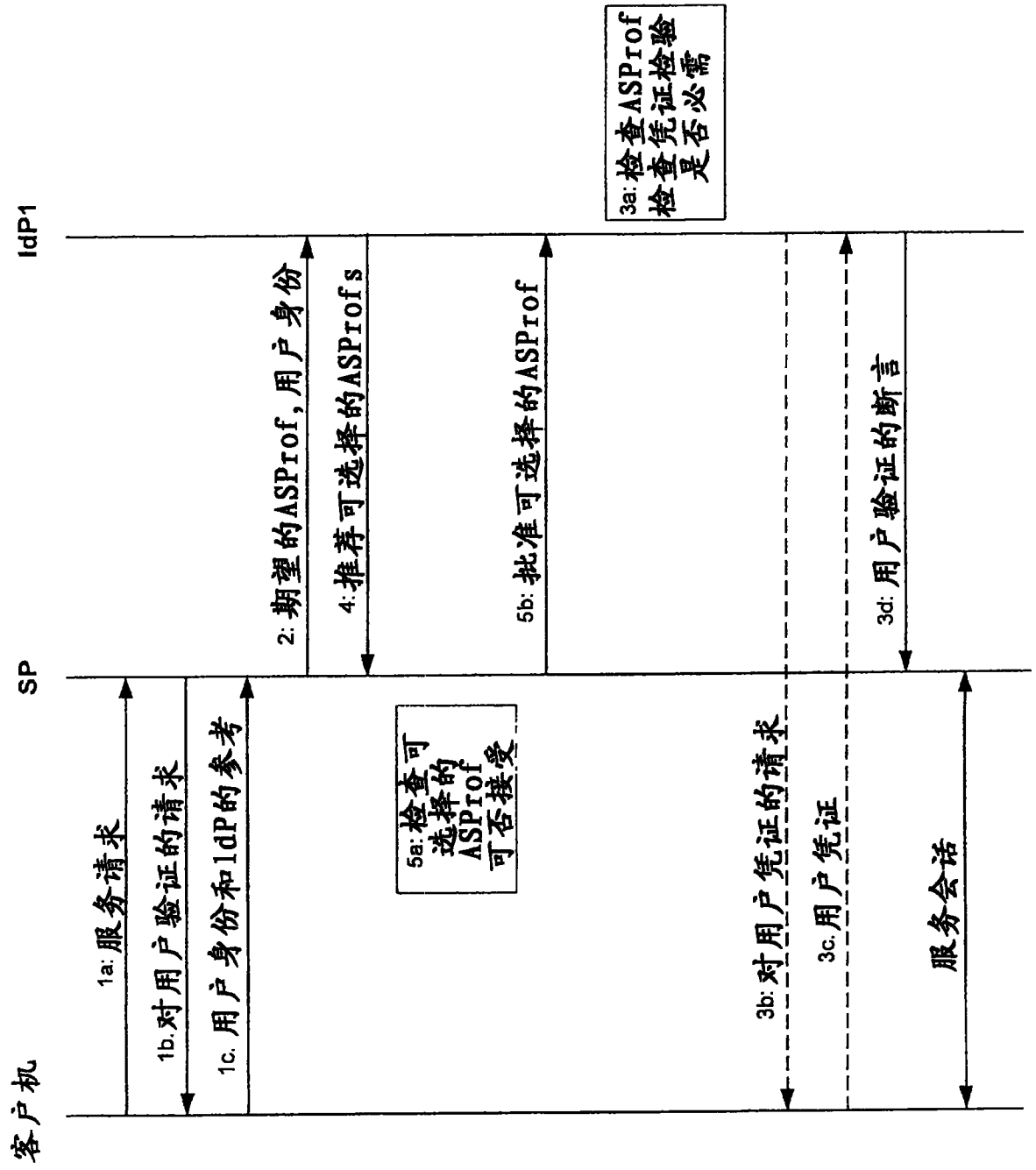

客户机
SP
IdP1
1a: 服务请求
1b. 对用户验证的请求
1c. 用户身份和IdP的参考
2: 期望的ASProf，用户身份
4: 推荐可选择的ASProfs
5a: 检查可选择的ASProf可否接受
5b: 批准可选择的ASProf
3a: 检查ASProf检查凭证检验是否必需
3b: 对用户凭证的请求
3c. 用户凭证
3d: 用户验证的断言
服务会话

图 5

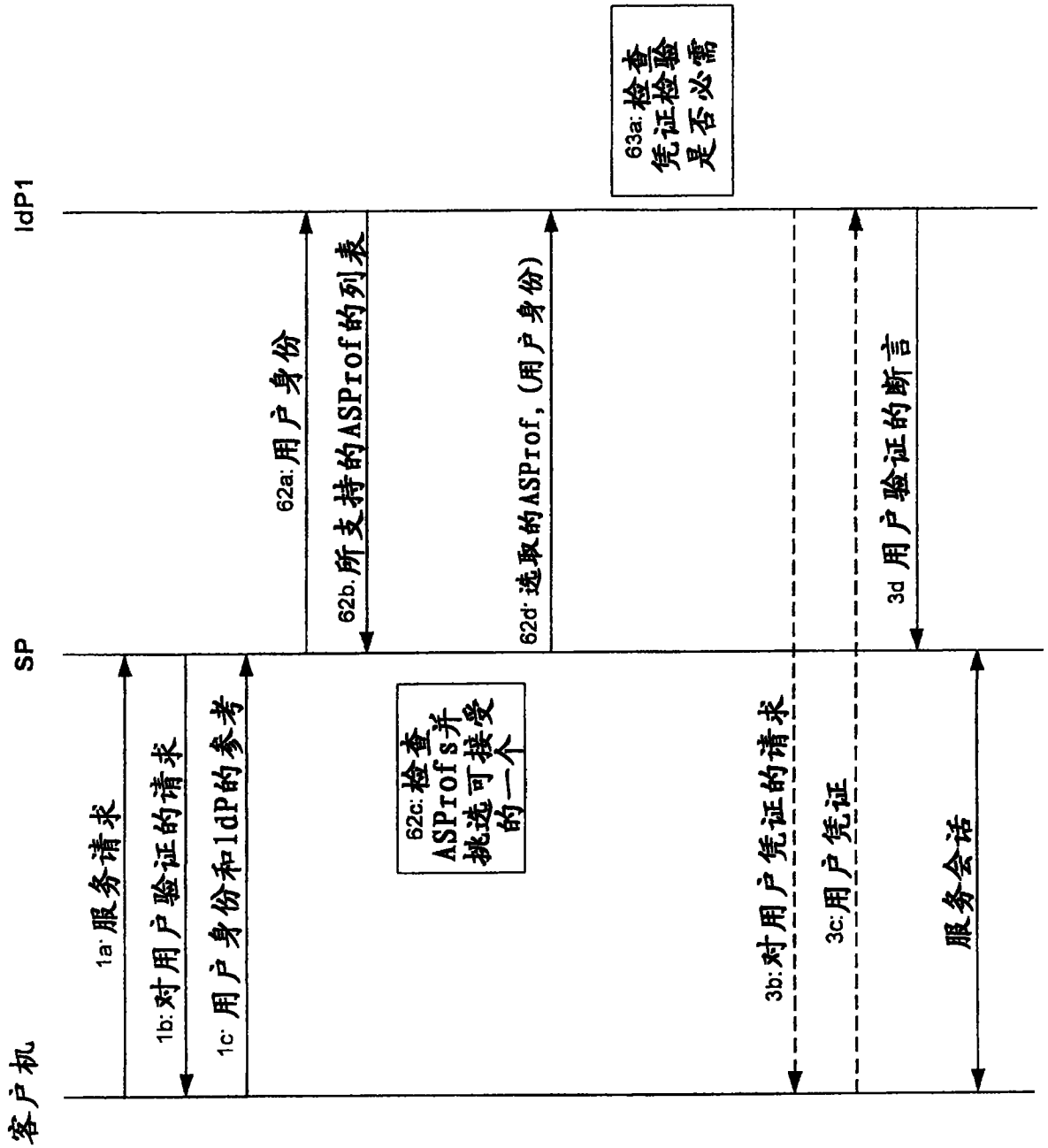

客户机
SP
IdP1
1a: 服务请求
1b: 对用户验证的请求
1c: 用户身份和IdP的参考
62a: 用户身份
62b. 所支持的ASProf的列表
62c: 检查ASProfs并挑选可接受的一个
62d: 选取的ASProf，(用户身份)
63a: 检查凭证检验是否必需
3b: 对用户凭证的请求
3c: 用户凭证
3d 用户验证的断言
服务会话

图 6

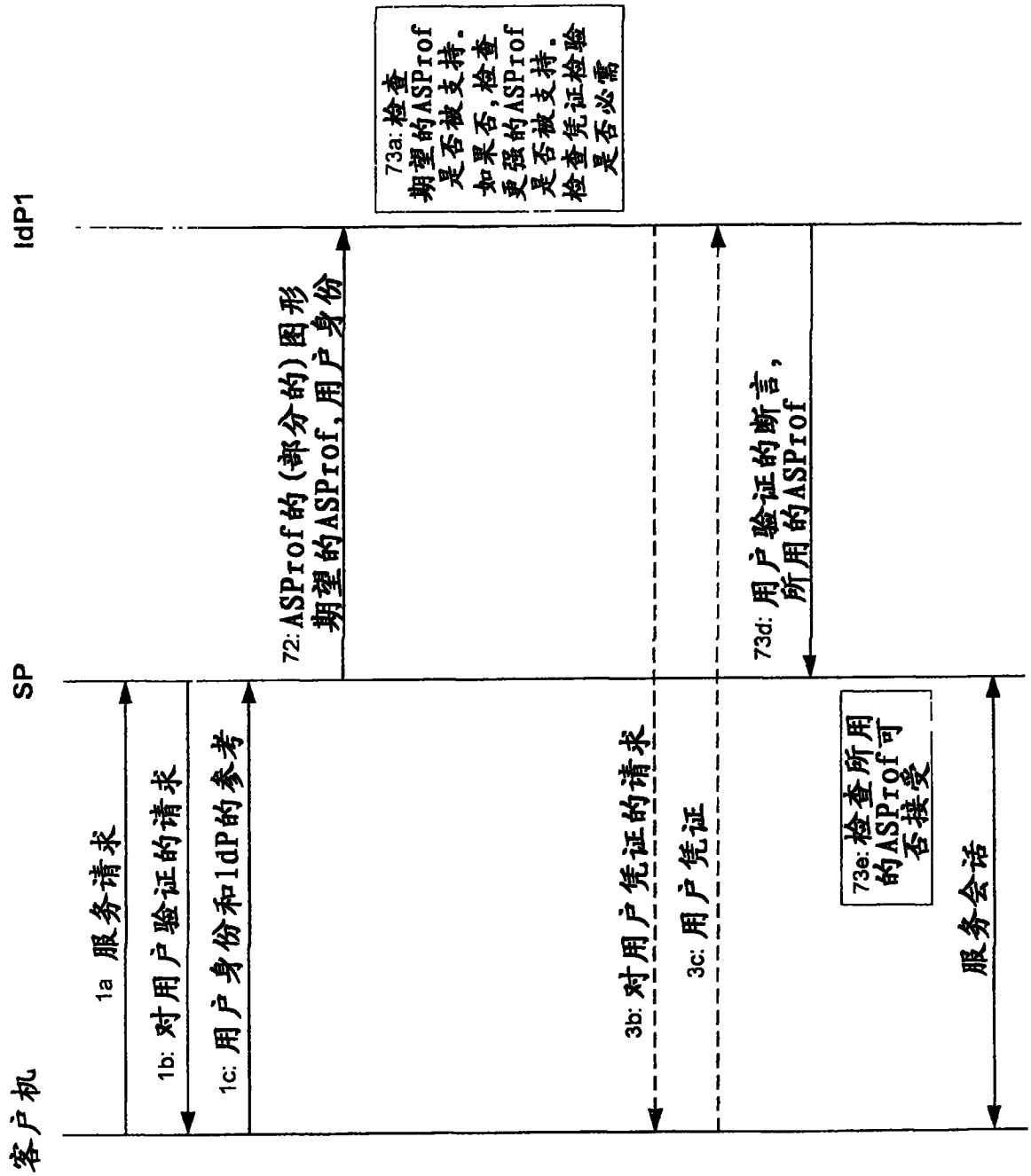

客户机
SP
IdP1
1a 服务请求
1b: 对用户验证的请求
1c: 用户身份和IdP的参考
72: ASProf的(部分的)图形
期望的ASProf，用户身份
73a: 检查
期望的ASProf
是否被支持.
如果否，检查
更强的ASProf
是否被支持.
检查凭证检验
是否必需
3b: 对用户凭证的请求
3c: 用户凭证
73d: 用户验证的断言，
所用的ASProf
73e: 检查所用
的ASProf可
否接受
服务会话

图 7

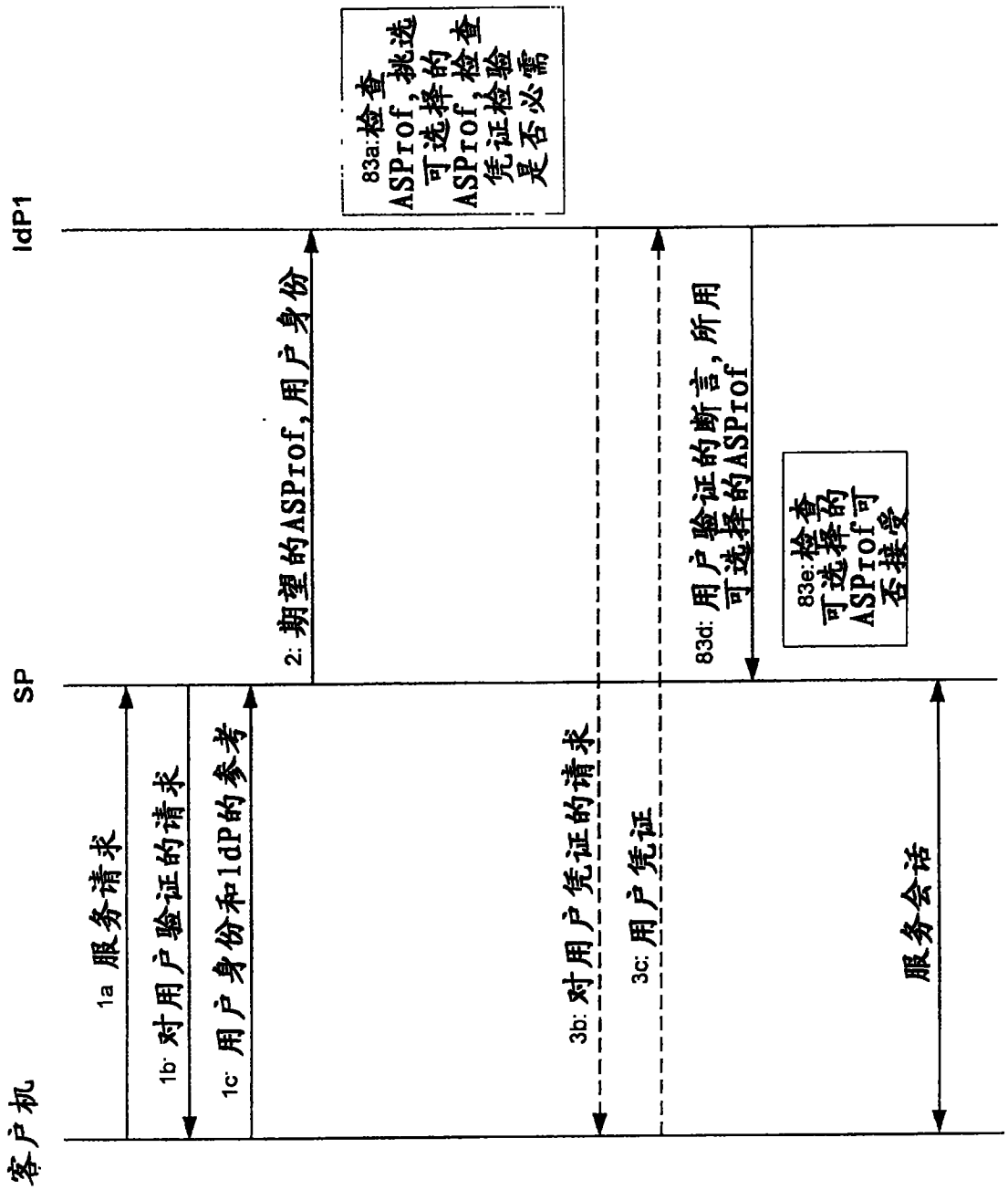

客户机
SP
IdP1
1a 服务请求
1b' 对用户验证的请求
1c' 用户身份和IdP的参考
2: 期望的ASPTof,用户身份
83a:检查ASPTof,挑选可选择的ASPTof,检查凭证检验是否必需
3b: 对用户凭证的请求
3c: 用户凭证
83d: 用户验证的断言,所用可选择的ASPTof
83e:检查可选择的ASPTof可否接受
服务会话

图 8

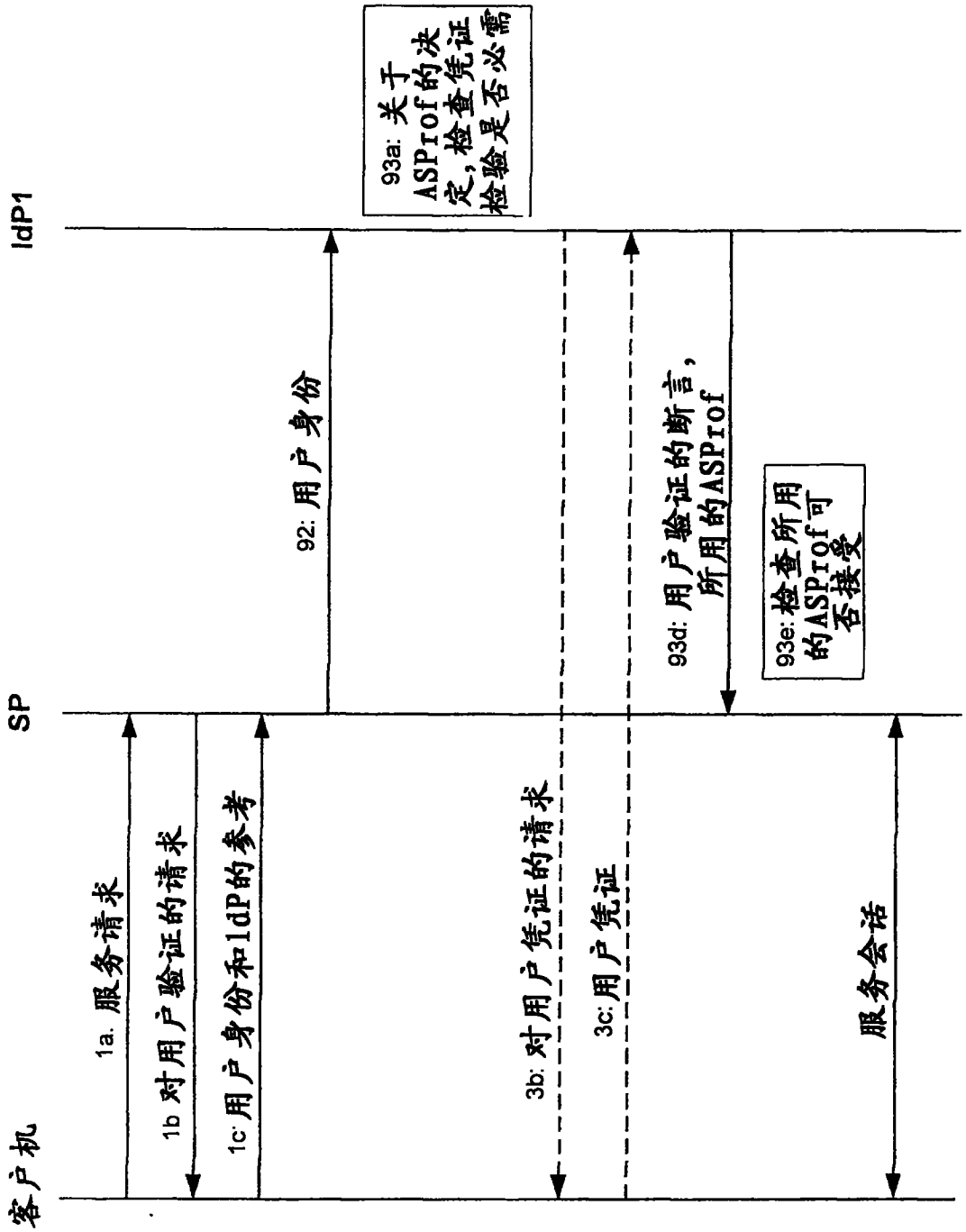

客户机
SP
IdP1
1a. 服务请求
1b 对用户验证的请求
1c 用户身份和IdP的参考
92: 用户身份
93a: 关于ASProf的决定，检查凭证检验是否必需
3b: 对用户凭证的请求
3c: 用户凭证
93d: 用户验证的断言，所用的ASProf
93e: 检查所用的ASProf可否接受
服务会话

图 9

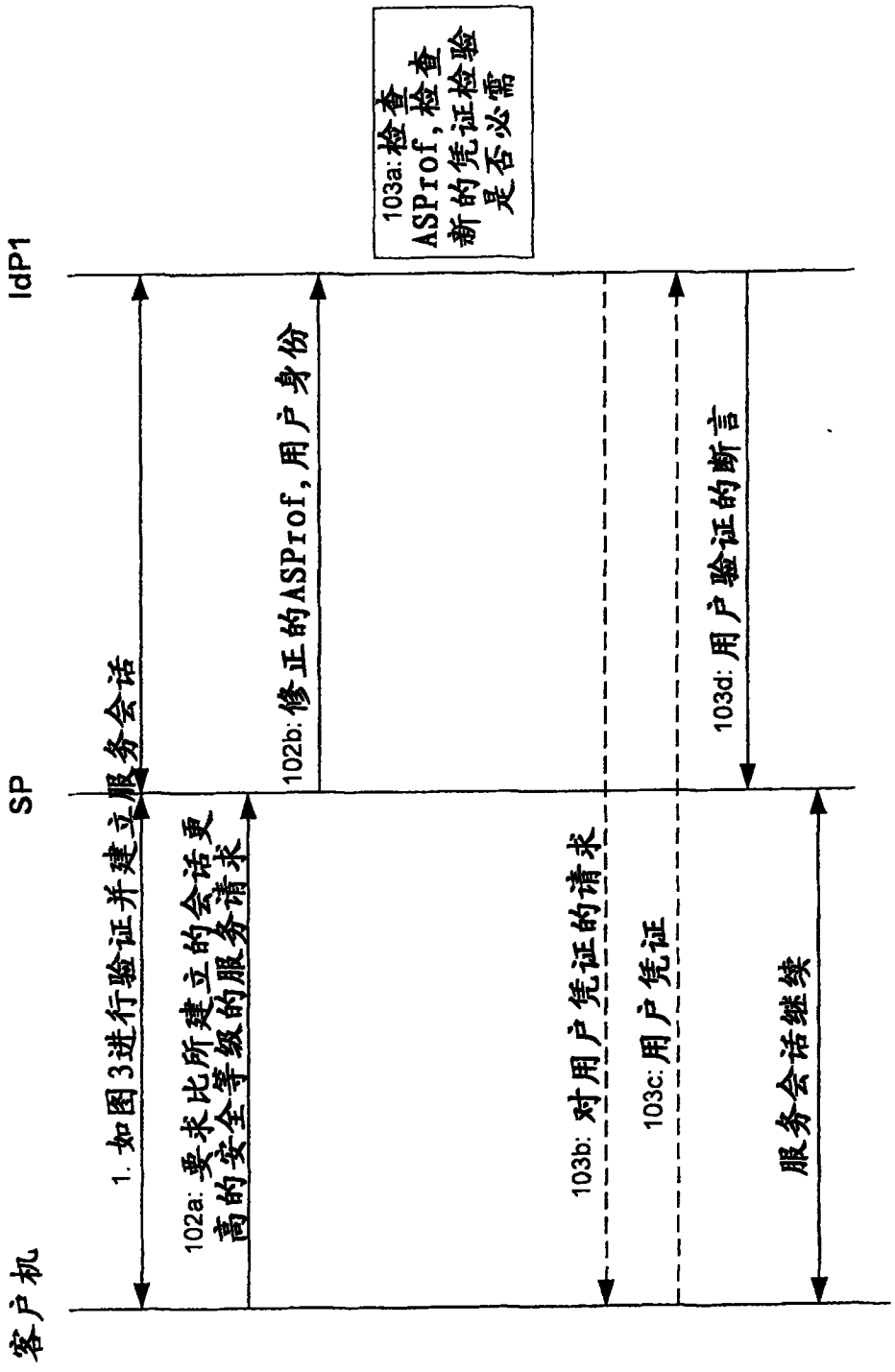

客户机
SP
IdP1
1. 如图3进行验证并建立服务会话
102a: 要求比所建立的会话更高的安全等级的服务请求
102b: 修正的ASProf，用户身份
103a: 检查ASProf，检查新的凭证检验是否必需
103b: 对用户凭证的请求
103c: 用户凭证
103d: 用户验证的断言
服务会话继续

图 10

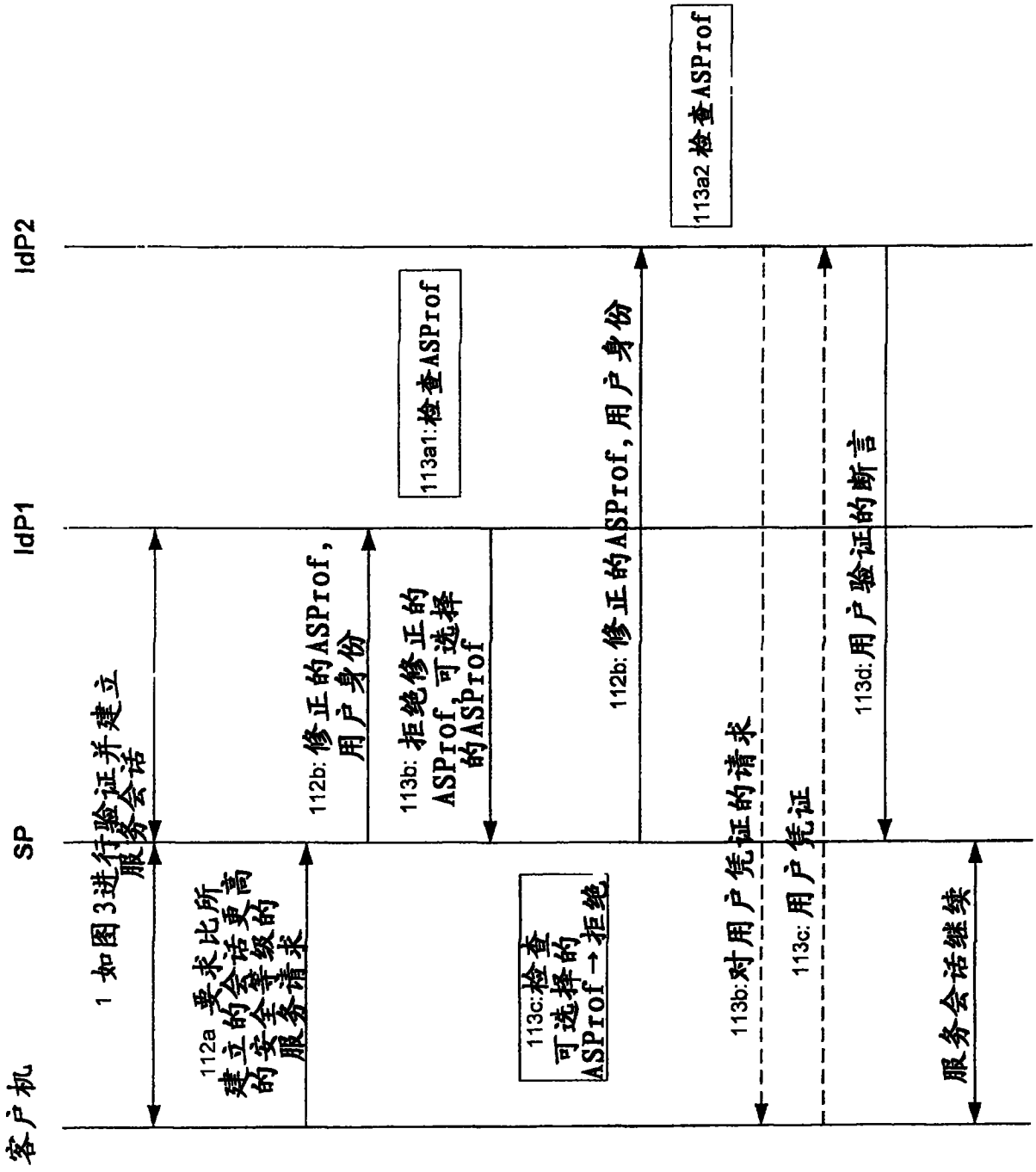

客户机
SP
IdP1
IdP2
1 如图3进行验证并建立服务会话
112a 要求比所建立的会话更高的安全等级的服务请求
112b: 修正的ASProf，用户身份
113b: 拒绝修正的ASProf，可选择的ASProf
113a1:检查ASProf
113c:检查可选择的ASProf→拒绝
112b: 修正的ASProf，用户身份
113a2 检查ASProf
113b:对用户凭证的请求
113c: 用户凭证
113d:用户验证的断言
服务会话继续

图 11

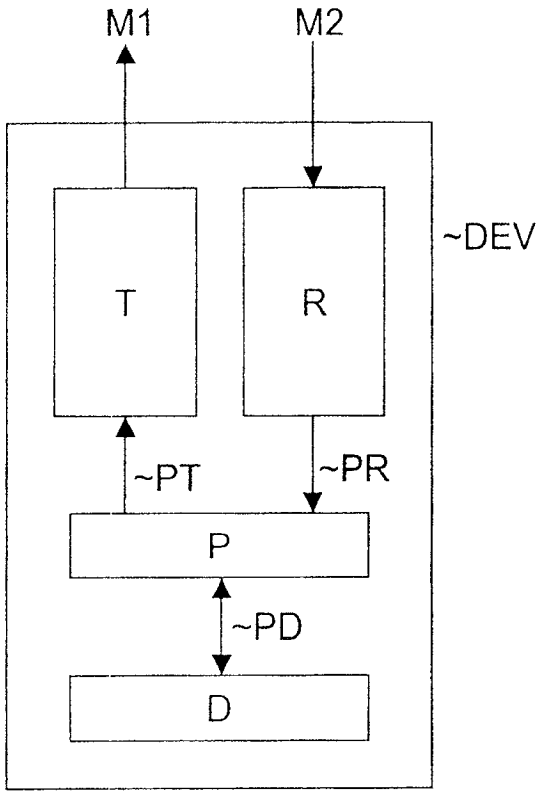


图 12

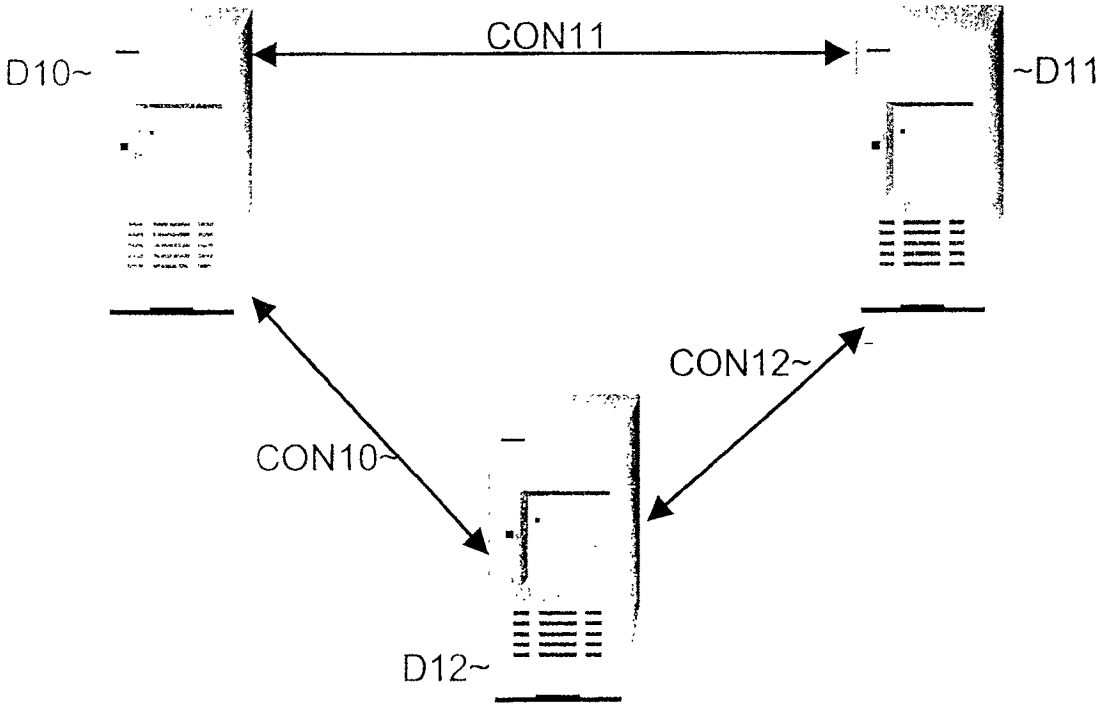


图 13

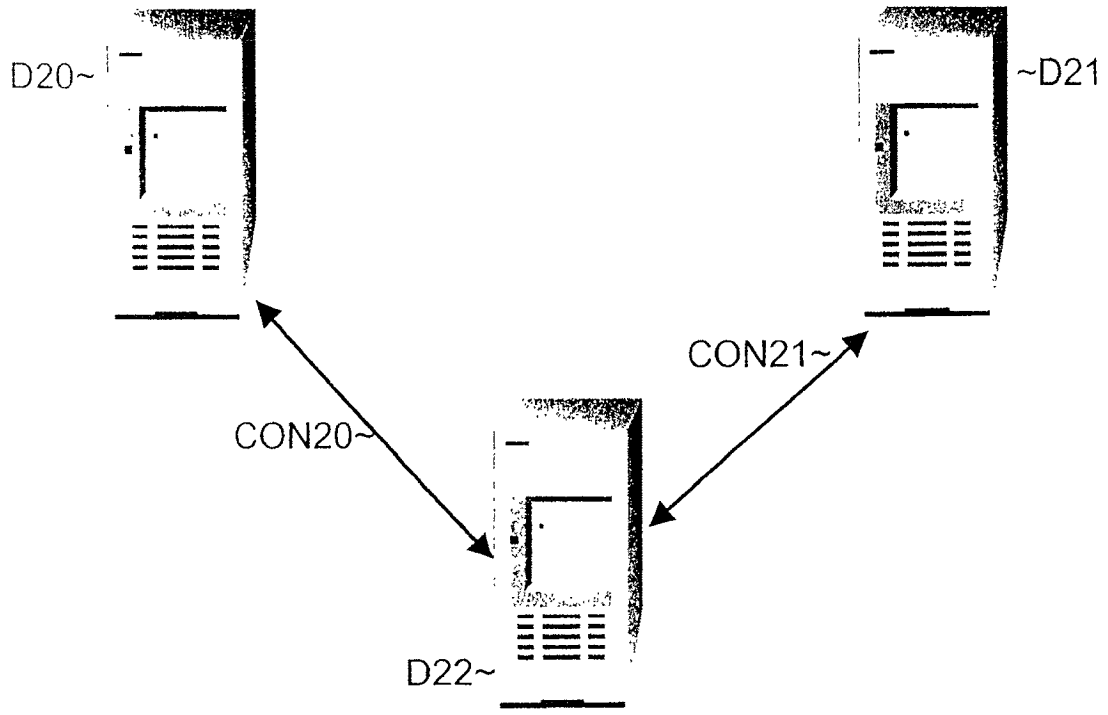

D20~
~D21
CON21~
CON20~
D22~

图 14

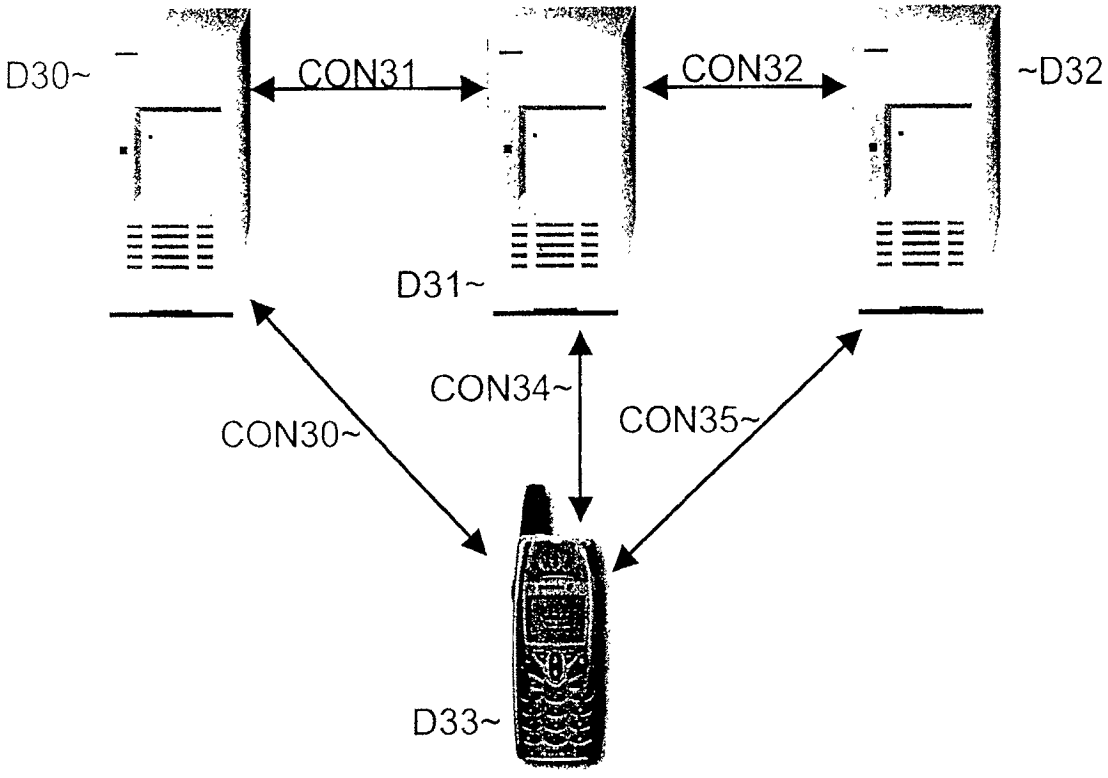

D30~
CON31
CON32
~D32
D31~
CON34~
CON30~
CON35~
D33~

图 15